

日本国特許庁
JAPAN PATENT OFFICE

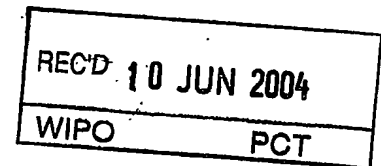
14.4.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 4月24日

出願番号
Application Number: 特願2003-119973
[ST. 10/C]: [JP2003-119973]



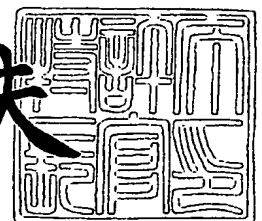
出願人
Applicant(s): 松下電器産業株式会社

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2004年 5月28日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 2022550083

【提出日】 平成15年 4月24日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 5/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山道 将人

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 布田 裕一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 館林 誠

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 パラメータ生成装置、パラメータ変換装置、暗号化システム、復号化システム、暗号装置、復号装置、暗号化方法、復号化方法、及びコンピュータ読取可能な記録媒体

【特許請求の範囲】

【請求項 1】 外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部と、

を備えることを特徴とする、パラメータ生成装置。

【請求項 2】 前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項 1 に記載のパラメータ生成装置。

【請求項 3】 前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする、請求項 2 に記載のパラメータ生成装置。

【請求項 4】 前記仮パラメータ組及び前記出力パラメータは、NTRU 暗号における次元 N 、非負整数 p 、非負整数 q 、秘密鍵多項式 f における係数の値が 1 となる係数の数を規定する非負整数 d_f 、公開鍵多項式を生成するとき用いるランダム多項式 g の係数の値が 1 となる係数の数を規定する非負整数 d_g 、及び平文を暗号化する時に用いる乱数多項式 r の係数の値が 1 となる係数の数を規定する非負整数 d の組から構成されることを特徴とする、請求項 1 から請求項 3 のいずれか 1 項に記載のパラメータ生成装置。

【請求項 5】 前記仮パラメータ生成部は、初期安全性決定情報を保持する初期安全性決定情報保持手段を備え、前記安全性レベル情報と前記初期安全性決定情報に基づいて前記仮パラメータ組に含まれる前記次元 N を生成することを特徴とする、請求項 4 に記載のパラメータ生成装置。

【請求項 6】 前記仮パラメータ生成部は、前記安全性レベル情報と前記次元 N に基づいて前記仮パラメータ組に含まれる前記非負整数 d_f 、前記非負整数 d_g 、前記非負整数 d を生成することを特徴とする、請求項 4 または請求項 5 に記載のパラメータ生成装置。

【請求項 7】 前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ組に含まれる前記非負整数 q を生成することを特徴とする、請求項 4 から請求項 6 のいずれか 1 項に記載のパラメータ生成装置。

【請求項 8】 前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元 N を生成することを特徴とする、請求項 4 から請求項 7 のいずれか 1 項に記載のパラメータ生成装置。

【請求項 9】 前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする、請求項 1 から請求項 8 のいずれか 1 項に記載のパラメータ生成装置。

【請求項 10】 前記エラー条件情報は、前記非負整数 p 、前記非負整数 q 、前記非負整数 d 、前記非負整数 d_f に対し、復号エラーが発生しないための条件を表す条件式

$$2 \cdot p \cdot d + 2 d_f - 1 < q / 2$$

であることを特徴とする、請求項 1 から請求項 9 のいずれか 1 項に記載のパラメータ生成装置。

【請求項 11】 前記出力パラメータ生成部は、1 つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、

前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特徴とする、請求項 2 から請求項 10 のいずれか 1 項に記載のパラメータ生成装置。

【請求項 12】 前記出力パラメータ生成部は、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする、請求項 11 に記載のパラメータ生成装置。

【請求項 13】 前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項 11 に記載のパラメータ生成装置。

【請求項 14】 前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数 d g を変更して前記変更仮パラメータ組を生成することを特徴とする、請求項 13 に記載のパラメータ生成装置。

【請求項 15】 外部から入力された安全性レベル情報に基づき、外部から入力された NTRU 暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置であって、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部と、

を備えることを特徴とする、パラメータ変換装置。

【請求項 16】 前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項 15 に記載のパラメータ変換装置。

【請求項 17】 前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする、請求項 16 に記載のパラメータ変換装置。

【請求項 18】 前記仮パラメータ組及び前記出力パラメータは、NTRU 暗号における次元 N 、非負整数 p 、非負整数 q 、秘密鍵多項式 f における係数の値が 1 となる係数の数を規定する非負整数 d_f 、公開鍵多項式を生成するとき用いるランダム多項式 g の係数の値が 1 となる係数の数を規定する非負整数 d_g 、及び平文を暗号化する時に用いる乱数多項式 r の係数の値が 1 となる係数の数を規定する非負整数 d の組から構成されることを特徴とする、請求項 15 から請求項 17 のいずれか 1 項に記載のパラメータ変換装置。

【請求項 19】 前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ組に含まれる前記非負整数 q を生成することを特徴とする、請求項 18 に記載のパラメータ変換装置。

【請求項 20】 前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元 N を生成することを特徴とする、請求項 18 または請求項 19 に記載のパラメータ変換装置。

【請求項 21】 前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする、請求項 15 から請求項 20 のいずれか 1 項に記載のパラメータ変換装置。

【請求項 22】 前記エラー条件情報は、前記非負整数 p 、前記非負整数 q 、前記非負整数 d 、前記非負整数 d_f に対し、復号エラーが発生しないための条件を表す条件式

$$2 \cdot p \cdot d + 2 \cdot d_f - 1 < q / 2$$

であることを特徴とする、請求項 15 から請求項 21 のいずれか 1 項に記載のパラメータ変換装置。

【請求項 23】 前記出力パラメータ生成部は、1 つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、

前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特

徴とする、請求項 16 から請求項 22 のいずれか 1 項に記載のパラメータ変換装置。

【請求項 24】 前記出力パラメータ生成部は、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする、請求項 23 に記載のパラメータ変換装置。

【請求項 25】 前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項 23 に記載のパラメータ変換装置。

【請求項 26】 前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数 d_g を変更して前記変更仮パラメータ組を生成することを特徴とする、請求項 25 に記載のパラメータ変換装置。

【請求項 27】 外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU 暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号化システムであって、

前記パラメータ生成装置は、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする、暗号化システム。

【請求項 28】 外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU 暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、

前記パラメータ生成装置は、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする、暗号化システム。

【請求項 29】 外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、

前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、

前記復号装置から前記出力パラメータに基づいて生成された NTRU 暗号の暗号鍵を受信する暗号鍵受信部と、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする、暗号装置。

【請求項 30】 外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して出力する暗号化方法であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいて NTRU 暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする、暗号化方法。

【請求項 31】 外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項32】 外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU暗号の復号鍵を生成して出力する鍵生成装置と、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、

前記パラメータ生成装置は、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出

力する復号化部を備えることを特徴とする、復号化システム。

【請求項 33】 暗号装置から受信した暗号文を N T R U 暗号で復号した復号文を生成して出力する復号装置であって、

前記暗号装置から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない N T R U 暗号のパラメータ組である出力パラメータを受信するパラメータ受信部と、

前記出力パラメータを入力として N T R U 暗号の暗号鍵と復号鍵を生成し出力する生成鍵出力部と、

前記暗号鍵を前記暗号装置へ送信する暗号鍵送信部と、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して前記復号文を生成して出力する復号文生成部を備えることを特徴とする、復号装置。

【請求項 34】 外部から入力された暗号文を N T R U 暗号で復号した復号文を生成して出力する復号化方法であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない N T R U 暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいて N T R U 暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする、復号化方法。

【請求項 35】 外部から入力された暗号文を N T R U 暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてNTRU暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項36】 外部から入力された安全性レベル情報に基づき、外部から入力されたNTRU暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置と、NTRU暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号システムであって、

前記パラメータ変換装置は、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力す

る暗号化部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする、暗号システム。

【請求項 37】 外部から入力された安全性レベル情報に基づき、外部から入力された NTRU 暗号のパラメータ組である入力パラメータと、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU 暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、

前記パラメータ生成装置は、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする、暗号化システム。

【請求項 38】 外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、

予め与えられた NTRU 暗号のパラメータ組である入力パラメータと予め与え

られた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、

前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、

前記復号装置から前記出力パラメータに基づいて生成されたNTRU暗号の暗号鍵を受信する暗号鍵受信部と、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする、暗号装置。

【請求項39】 外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号化方法であって、

予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする、暗号化方法。

【請求項40】 外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与え

られた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項 41】 外部から入力された安全性レベル情報に基づき、外部から入力されたNTRU暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU暗号の復号鍵を生成して出力する鍵生成装置と、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、

前記パラメータ生成装置は、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする、復号化システム。

【請求項 4 2】 外部から入力された暗号文を N T R U 暗号で復号した復号文を生成して出力する復号化方法であって、

予め与えられた N T R U 暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない N T R U 暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいて N T R U 暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする、復号化方法。

【請求項 4 3】 外部から入力された暗号文を N T R U 暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられた N T R U 暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない N T R U 暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいて N T R U 暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を

生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、NTRU暗号のパラメータ生成に関するものである。

【0002】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献1参照）。この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータ内容を上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信内容データを受信する。そして、受信装置は、暗号化された通信内容データを、自身の有する秘密鍵で復号して元の通信内容データを得る。

【0003】

なお、暗号は、送信装置と受信装置との間の秘匿通信を目的とするものであり、第三者による暗号解読に対する安全性が重要なのは言うまでもない。公開鍵暗号では、暗号化された通信内容データ（以降、暗号文と記述）から、通信内容データ（以降、平文と記述）が解読される可能性と、受信装置が秘密に保持し、暗号文から平文を得る際に用いる秘密鍵が解読される可能性がある。一般に、公開鍵暗号では、第三者によるこれらの暗号解読の解読時間が十分に大きく（例えば、最新のコンピュータを用いて1000年かかる等）、現実的な時間内では解読

できないことが求められる。

【0004】

1996年、高速処理が可能な公開鍵暗号として、NTRU暗号が提案された（例えば、非特許文献2参照）。このNTRU暗号については、非特許文献2に詳細が記載されているのでここでは詳細な説明を省略するが、ある法の下でべき乗剰余演算を行うRSA暗号や楕円曲線上の点のスカラ倍演算を行う楕円曲線暗号に比べ、高速に演算可能な多項式演算で暗号化と復号化を行うので、従来の公開鍵暗号よりもソフトウェアにより高速に処理することが可能である。

【0005】

従って、公開鍵暗号にNTRU暗号を用いた暗号システムでは、従来の公開鍵暗号を用いた暗号システムよりも、送信装置及び受信装置の処理が高速に行えるという利点がある。

【0006】

なお、このNTRU暗号を用いて実際に暗号化や復号化を行うためには、非負整数のパラメータ、 N 、 p 、 q 、 df 、 dg 、 d が必要であり（例えば、非特許文献2参照）、現在、これらのパラメータの具体的な値が提示されている（例えば、非特許文献5参照）。

【0007】

このNTRU暗号は、第三者による平文や秘密鍵の暗号解読方法として、これらを総当りで探索する暗号解読と、LLLアルゴリズムを用いて解読する暗号解読がある（例えば、非特許文献2参照）が、非特許文献5に提示されたパラメータを用いれば、これらの暗号解読の解読時間は十分に大きく、NTRU暗号は安全であることが示されている（例えば、非特許文献3、非特許文献4、非特許文献5参照）。

【0008】

一方、このNTRU暗号は、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成しても、復号文が元の平文と異なる場合が発生する（例えば、非特許文献2参照）。このことを復号エラーが発生するという。この復号エラーはNTRU暗号のパラメータにより、その

発生確率が異なる（例えば、非特許文献5参照）。

【0009】

この復号エラーに関し、非特許文献2には、復号エラーが発生しないためには、NTRU暗号の公開鍵多項式 h を生成するときに用いるランダム多項式 g 、乱数多項式 r 、平文多項式 m 、秘密鍵多項式 f の演算結果の多項式 $(p \cdot r \times g + f \times m)$ の係数の値が $-q/2$ から $q/2$ に入ることが必要であることが示されている。しかし、このようにNTRU暗号のパラメータを選んだときの暗号解読に対する解読時間については不明であり、暗号解読に対して安全でかつ復号エラーが発生しないNTRU暗号のパラメータは知られていない。

【0010】

【非特許文献1】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997。

【非特許文献2】

Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.

【非特許文献3】

Joseph H. Silverman, "NTRU Cryptosystems Technical Report #012, Estimated Breaking Times for NTRU Lattices", [online]、1999年3月9日、[2003年2月18日検索]、インターネット<URL: <http://www.ntru.com/cryptolab/pdf/NTRUTech012.pdf>>

【非特許文献4】

Joseph H. Silverman, "NTRU Cryptosystems Technical Report #013, Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem", [online]、1999年3月9日、[2003年2月18日検索]、インターネット<URL: <http://www.ntru.com/cryptolab/pdf/NTRUTech013.pdf>>

【非特許文献5】

Joseph H. Silverman, "NTRU Cryptosystems Technical Report #011, Wraps, Gaps, and Lattice Constants", [online], 1999年1月21日、[2003年4月18日検索]、インターネット<URL: <http://www.ntru.com/cryptolab/pdf/NTRUTech011#v2.pdf>>

【0011】

【発明が解決しようとする課題】

上述したように、高速処理が可能なNTRU暗号では、復号エラーが発生すると、受信装置が、送信装置の暗号化した平文を正しく得られない場合がある。すなわち、送信装置と受信装置との間で確実な暗号化通信ができないことになる。

【0012】

暗号システムにおいては、平文を相手に正しく伝えることが重要なのは言うまでもない。また、暗号は、第三者による暗号解読に対する安全性が重要なのは言うまでもない。

【0013】

しかしながら、従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータを生成するための条件が知られておらず、そのようなNTRU暗号のパラメータを生成できない。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができない。

【0014】

そこで、本発明は上記の課題に鑑み、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータを生成するパラメータ生成装置を提供することを第1の目的とする。

【0015】

また、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、入力されたNTRU暗号のパラメータに対し、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータに変換するパラメータ変換装置を提供することを第2の目的とする。

【0016】

また、これらのパラメータ装置もしくはパラメータ変換装置により生成されたパラメータを用いて、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができる、暗号システム、暗号装置及び復号装置を提供することを第3の目的とする。

【0017】

【課題を解決するための手段】

上記課題を解決するために、請求項1における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部とを備えることを特徴とする。

【0018】

請求項2における発明は、請求項1に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【0019】

請求項3における発明は、請求項2に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする。

【0020】

請求項4における発明は、請求項1から請求項3のいずれか1項に記載のパラメータ生成装置において、前記仮パラメータ組及び前記出力パラメータは、NTRU暗号における次元 N 、非負整数 p 、非負整数 q 、秘密鍵多項式 f における係数の値が1となる係数の数を規定する非負整数 d_f 、公開鍵多項式を生成すると

きに用いるランダム多項式 g の係数の値が 1 となる係数の数を規定する非負整数 d_g 、及び平文を暗号化する時に用いる乱数多項式 r の係数の値が 1 となる係数の数を規定する非負整数 d の組から構成されることを特徴とする。

【0021】

請求項 5 における発明は、請求項 4 に記載のパラメータ生成装置において、前記仮パラメータ生成部は、初期安全性決定情報を保持する初期安全性決定情報保持手段を備え、前記安全性レベル情報と前記初期安全性決定情報に基づいて前記仮パラメータ組に含まれる前記次元 N を生成することを特徴とする。

【0022】

請求項 6 における発明は、請求項 4 または請求項 5 に記載のパラメータ生成装置において、前記仮パラメータ生成部は、前記安全性レベル情報と前記次元 N に基づいて前記仮パラメータ組に含まれる前記非負整数 d_f 、前記非負整数 d_g 、前記非負整数 d を生成することを特徴とする。

【0023】

請求項 7 における発明は、請求項 4 から請求項 6 のいずれか 1 項に記載のパラメータ生成装置において、前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ組に含まれる前記非負整数 q を生成することを特徴とする。

【0024】

請求項 8 における発明は、請求項 4 から請求項 7 のいずれか 1 項に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元 N を生成することを特徴とする。

【0025】

請求項 9 における発明は、請求項 1 から請求項 8 のいずれか 1 項に記載のパラメータ生成装置において、前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする。

【0026】

請求項 10 における発明は、請求項 1 から請求項 9 のいずれか 1 項に記載のパ

ラメータ生成装置において、前記エラー条件情報は、前記非負整数 p 、前記非負整数 q 、前記非負整数 d 、前記非負整数 d_f に対し、復号エラーが発生しないための条件を表す条件式 $2 \cdot p \cdot d + 2 d_f - 1 < q / 2$ であることを特徴とする。

【0027】

請求項 11 における発明は、請求項 2 から請求項 10 のいずれか 1 項に記載のパラメータ生成装置において、前記出力パラメータ生成部は、1 つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特徴とする。

【0028】

請求項 12 における発明は、請求項 11 に記載のパラメータ生成装置は、前記出力パラメータ生成部において、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする。

【0029】

請求項 13 における発明は、請求項 11 に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【0030】

請求項 14 における発明は、請求項 13 に記載のパラメータ生成装置において、前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数 d_g を変更して前記変更仮パラメータ組を生成することを特徴とする。

【0031】

請求項 15 における発明は、外部から入力された安全性レベル情報に基づき、外部から入力された NTRU 暗号のパラメータ組である入力パラメータを、前記

安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置であって、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部と、を備えることを特徴とする。

【0032】

請求項16における発明は、請求項15に記載のパラメータ変換装置において、前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【0033】

請求項17における発明は、請求項16に記載のパラメータ変換装置において、前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする。

【0034】

請求項18における発明は、請求項15から請求項17のいずれか1項に記載のパラメータ変換装置において、前記仮パラメータ組及び前記出力パラメータは、NTRU暗号における次元 N 、非負整数 p 、非負整数 q 、秘密鍵多項式 f における係数の値が1となる係数の数を規定する非負整数 d_f 、公開鍵多項式を生成するときに用いるランダム多項式 g の係数の値が1となる係数の数を規定する非負整数 d_g 、及び平文を暗号化する時に用いる乱数多項式 r の係数の値が1となる係数の数を規定する非負整数 d の組から構成されることを特徴とする。

【0035】

請求項19における発明は、請求項18に記載のパラメータ変換装置において、前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ

組に含まれる前記非負整数 q を生成することを特徴とする。

【0036】

請求項 20 における発明は、請求項 18 または請求項 19 に記載のパラメータ変換装置において、前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元 N を生成することを特徴とする。

【0037】

請求項 21 における発明は、請求項 15 から請求項 20 のいずれか 1 項に記載のパラメータ変換装置において、前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする。

【0038】

請求項 22 における発明は、請求項 15 から請求項 21 のいずれか 1 項に記載のパラメータ変換装置において、前記エラー条件情報は、前記非負整数 p 、前記非負整数 q 、前記非負整数 d 、前記非負整数 d_f に対し、復号エラーが発生しないための条件を表す条件式 $2 \cdot p \cdot d + 2 \cdot d_f - 1 < q / 2$ であることを特徴とする。

【0039】

請求項 23 における発明は、請求項 16 から請求項 22 のいずれか 1 項に記載のパラメータ変換装置において、前記出力パラメータ生成部は、1 つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特徴とする。

【0040】

請求項 24 における発明は、請求項 23 に記載のパラメータ変換装置において、前記出力パラメータ生成部は、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする。

【0041】

請求項 25 における発明は、請求項 23 に記載のパラメータ変換装置において

、前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【0042】

請求項 26 における発明は、請求項 25 に記載のパラメータ変換装置において、前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数 d_g を変更して前記変更仮パラメータ組を生成することを特徴とする。

【0043】

請求項 27 における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しない NTRU 暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU 暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文を NTRU 暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号化システムであって、前記パラメータ生成装置は、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【0044】

請求項28における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、前記パラメータ生成装置は、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする。

【0045】

請求項29における発明は、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、前記復号装置から前記出力パラメータに基づいて生成されたNTRU暗号の暗号鍵を受信する暗号鍵受信部と、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して

前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする。

【0046】

請求項30における発明は、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号化方法であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする。

【0047】

請求項31における発明は、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【0048】

請求項32における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU暗号の復号鍵を生成して出力する鍵生成装置と、外部から入

力された暗号文をNTRU暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、前記パラメータ生成装置は、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【0049】

請求項33における発明は、暗号装置から受信した暗号文をNTRU暗号で復号した復号文を生成して出力する復号装置であって、前記暗号装置から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを受信するパラメータ受信部と、前記出力パラメータを入力としてNTRU暗号の暗号鍵と復号鍵を生成し出力する生成鍵出力部と、前記暗号鍵を前記暗号装置へ送信する暗号鍵送信部と、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して前記復号文を生成して出力する復号文生成部を備えることを特徴とする。

【0050】

請求項34における発明は、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力する復号化方法であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成

して出力するステップと、前記出力パラメータに基づいてNTRU暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする。

【0051】

請求項35における発明は、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【0052】

請求項36における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたNTRU暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置と、NTRU暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号システムであって、前記パラメータ変換装置は、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パ

ラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【0053】

請求項37における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたNTRU暗号のパラメータ組である入力パラメータと、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、前記パラメータ生成装置は、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする。

【0054】

請求項38における発明は、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発

生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、前記復号装置から前記出力パラメータに基づいて生成されたNTRU暗号の暗号鍵を受信する暗号鍵受信部と、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする。

【0055】

請求項39における発明は、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力する暗号化方法であって、予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする。

【0056】

請求項40における発明は、外部から入力された平文をNTRU暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えら

れた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【0057】

請求項41における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたNTRU暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、NTRU暗号の復号鍵を生成して出力する鍵生成装置と、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、前記パラメータ生成装置は、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【0058】

請求項42における発明は、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力する復号化方法であって、予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を

生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする。

【0059】

請求項43における発明は、外部から入力された暗号文をNTRU暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられたNTRU暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてNTRU暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【0060】

【発明の実施の形態】

以下、本発明に係るパラメータ生成装置及びパラメータ変換装置の実施の形態について、図面を用いて説明する。

【0061】

本発明に係るパラメータ生成装置及びパラメータ変換装置は、NTRU暗号のパラメータを扱う。このNTRU暗号については、非特許文献2に詳しく述べられているので、ここでは詳細な説明を省略するが、以下に簡単に説明する。

【0062】

(1) NTRU暗号のパラメータ

NTRU暗号は、非負整数のパラメータ、 N 、 p 、 q 、 df 、 dg 、 d を持つ。非特許文献2には、NTRU暗号のパラメータの例として、 $(N, p, q, df, dg, d) = (107, 3, 64, 15, 12, 5)$ 、 $(N, p, q, df, dg, d) = (167, 3, 128, 61, 20, 18)$ 、 $(N, p, q, df, dg, d) = (503, 3, 256, 216, 72, 55)$ の3つの例が挙げられている。

【0063】

以下に、これらのパラメータの意味を説明する。

【0064】

(i) パラメータ N

NTRU暗号は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。NTRU暗号で扱う多項式の次元は、上記パラメータ N により決まる。

【0065】

NTRU暗号で扱う多項式は、上記パラメータ N に対し、 $N-1$ 次元以下の整数係数多項式であり、例えば $N=5$ のとき、 $X^4 + X^3 + 1$ 等の多項式である。ここで、「 X^a 」は X の a 乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵 h 、秘密鍵 f 、平文 m 、乱数 r 、暗号文 c はいずれも、 $N-1$ 次元以下の多項式として表現される（以降、それぞれを公開鍵多項式 h 、秘密鍵多項式 f 、平文多項式 m 、乱数多項式 r 、暗号文多項式 c と呼ぶ）。

【0066】

そして、多項式演算は、上記パラメータ N に対し、 $X^N = 1$ という関係式を用いて、演算結果が常に $N-1$ 次元以下の多項式になるように演算される。例えば、 $N=5$ の場合、多項式 $X^4 + X^2 + 1$ と多項式 $X^3 + X$ の積は、多項式と多項式の積を \times 、整数と多項式の積（あるいは整数と整数の積）を \cdot とすると、 $X^5 = 1$ という関係から、

$$\begin{aligned} & (X^4 + X^2 + 1) \times (X^3 + X) \\ &= X^7 + 2 \cdot X^5 + 2 \cdot X^3 + X \end{aligned}$$

$$=X^2 \times 1 + 2 \cdot 1 + 2 \cdot X^3 + X$$

$$=2 \cdot X^3 + X^2 + X + 2$$

というように、常に $N-1$ 次元以下の多項式になるように演算される。

【0067】

(i i) パラメータ p 、 q

NTRU暗号では、非負整数のパラメータ p 、 q を用いる。非特許文献2に記載の通り、このパラメータ p 、 q は互いに素となる必要がある。

【0068】

(i i i) パラメータ df 、 dg 、 d

NTRU暗号で扱う秘密鍵多項式 f 、公開鍵多項式を生成するときに秘密鍵多項式 f と共に用いるランダム多項式 g 、及び平文を暗号化するときに用いる乱数多項式 r の選び方は、それぞれパラメータ df 、 dg 、 d により決まる。

【0069】

まず、秘密鍵多項式 f は、 df 個の係数が1であり、かつ $(df-1)$ 個の係数が-1であり、かつ他の係数は0となるように選ぶ。すなわち、乱数多項式 f は $N-1$ 次元以下の多項式であり、0次元(定数項)から $N-1$ 次元まで、 N 個の係数があるが、この N 個の係数のうち、 df 個の係数が1であり、かつ $(df-1)$ 個の係数が-1であり、かつ $(N-2df+1)$ 個の係数が0となるように選ぶ。

【0070】

そして、ランダム多項式 g は、 dg 個の係数が1であり、かつ dg 個の係数が-1であり、かつ他の係数は0となるように選ぶ。また、乱数多項式 r は、 d 個の係数が1であり、かつ d 個の係数が-1であり、かつ他の係数は0となるように選ぶ。

【0071】

(2) NTRU暗号の復号エラー

ところで、このNTRU暗号は、平文多項式 m を暗号化して暗号文多項式 c を生成したとき、暗号文多項式 c を復号して得られる復号文多項式 m' が平文多項式 m と異なる場合が発生する。この場合は、復号時に正しく平文多項式 m が得ら

れないことになる。このことを復号エラーが発生するという。

【0072】

非特許文献2には、公開鍵多項式 h の生成するときに用いるランダム多項式 g 、乱数多項式 r 、平文多項式 m 、秘密鍵多項式 f の演算結果の多項式 $(p \cdot r \times g + f \times m)$ のいずれかの次数の係数の値が $-q/2$ から $q/2$ の間に入らなかったとき、復号エラーが発生することが記載されている。非特許文献2に挙げられた上述の3つのパラメータにおいては、非特許文献5に記載の通り、小さい発生確率 (10^{-5} 程度) ではあるが復号エラーが発生してしまう。

【0073】

(実施の形態1)

本発明に係る実施の形態1としてのパラメータ生成装置1について説明する。

【0074】

<パラメータ生成装置1の概要>

最初に、図1を用いてパラメータ生成装置1の概要を説明する。

【0075】

このパラメータ生成装置1は、あるパラメータのNTRU暗号の格子強度係数 GL 、その格子強度係数 GL を持つNTRU暗号の解読時間評価式 EF 、復号エラーが発生しないパラメータの条件式 ED 、及び初期安全性決定式 IF が予め与えられている。

【0076】

そして、このパラメータ生成装置1は、外部より、NTRU暗号が達成すべき安全性レベルを示す安全性レベル情報 SLI を入力したとき、予め与えられている、格子強度係数 GL と解読時間評価式 EF と条件式 ED と初期安全性決定式 IF を用いて、総当りの探索による解読とLLLアルゴリズムによる解読に対し、入力された安全性レベル情報 SLI が示す安全性レベルを達成し、かつ復号エラーが発生しないNTRU暗号のパラメータ組 PS を生成して、外部へ出力する装置である。

【0077】

以上が、パラメータ生成装置1の概要であるが、以下に、格子強度係数 GL 、

解読時間評価式EF、条件式ED、初期安全性決定式IFの与え方について説明した後、パラメータ生成装置1の詳細について説明を行う。

【0078】

＜格子強度係数GL、解読時間評価式EF、条件式ED＞

ここでは、まず、格子強度係数GL、解読時間評価式EF、復号エラーが発生しないパラメータの条件式EDについてその内容を説明して、その与え方について説明する。

【0079】

(格子強度係数GLと解読時間評価式EF)

NTRU暗号における、LLLアルゴリズムを用いた解読時間Tの解読時間評価式EFは、NTRU暗号のパラメータdf、dg、qにより定まるものであって、パラメータdf、dg、qから計算される格子強度係数GLの値により類別される。非特許文献3には、格子強度係数GLが、NTRU暗号のパラメータdf、dg、qから、

$$GL = (4 \cdot \pi \cdot e \cdot |f| \cdot |g| / q)^{(0.5)}$$

のように導出されること、さらにその格子強度係数GLが一定ならば、そのようなパラメータdf、dg、qをもつNTRU暗号に対しては、ある定数A、Bが存在して、LLLアルゴリズムを用いた解読の解読時間TがパラメータNに対し次の解読時間評価式EFを満たすことが記載されている。

【0080】

$$EF: \log(T) \geq A \cdot N + B$$

ここで、 $\log(T)$ は解読時間Tの自然対数である。また、 π は円周率、 e は自然対数の底、 $|f|$ は秘密鍵多項式fのノルム、 $|g|$ はランダム多項式のノルムを表す。具体的には、 $|f| = (2 \cdot df - 1)^{(0.5)}$ 、 $|g| = (2 \cdot dg)^{(0.5)}$ である。

【0081】

なお、非特許文献3には、上記に説明した解読時間評価式EFにおける定数A、Bについて、パラメータNが小さいところでの解読時間Tを実測し、その実測データを用いて近似することによりその定数A、Bの値を導けることが記載され

ている。

【0082】

また、非特許文献4には、格子強度係数 GL の値が大きくなれば、LLLアルゴリズムを用いたNTRU暗号の解読は、より難しくなることが記載されている。従って、いま、ある格子強度係数 GL_1 の値に対し、格子強度係数 GL_1 がその値をとるようなパラメータ df 、 dg 、 q をもつNTRU暗号に対する、LLLアルゴリズムを用いた解読の解読時間 T の解読時間評価式 EF_1 が、

$$EF_1: \log(T) \geq A \cdot N + B \quad (A, B: \text{定数})$$

で与えられているとする。すると、以上の議論により、別のパラメータ df 、 dg 、 q から導出される格子強度係数 GL の値が、もし、上記の格子強度係数 GL_1 の値よりも大きければ、その別のパラメータ df 、 dg 、 q をもつNTRU暗号の解読時間 T は、少なくとも上記の解読時間評価式 EF_1 を満たすことが導ける。

【0083】

(復号エラーが発生しないパラメータの条件式 ED)

非特許文献2には、NTRU暗号の復号プロセスにおいて計算される多項式、 $p \cdot r \times g + f \times m$ の全ての係数が、 $-q/2$ から $q/2$ の範囲に収まっていれば、正しく復号処理を行うことができ、復号エラーが発生しないことが記載されている。

【0084】

(格子強度係数 GL と解読時間評価式 EF の与え方)

まず、パラメータ df 、 dg 、 q の値を決定する。ここでは、一例として、 $df=34$ 、 $dg=34$ 、 $q=512$ とする。そして、このパラメータ df 、 dg 、 q から上記格子強度係数 GL の値を計算し、その格子強度係数 GL を、予め式格納部110に与えておく。上記例では、格子強度係数 GL は $GL=2.12$ となる。

【0085】

次に、解読時間評価式 EF として、上記格子強度係数 GL の値に対し、その値をとるパラメータ df 、 dg 、 q をもつNTRU暗号の解読時間 T の解読時間評

価式EFを、以下のようにして求め、予め式格納部110に与えておく。

【0086】

すなわち、上記解読時間評価式EFは、パラメータdf、dg、qから計算される格子強度係数の値が2.12以上であるときに、LLLアルゴリズムを用いた解読の解読時間Tを、少なく見積もることなく評価できるものである。

【0087】

(i) パラメータNが小さいところでの解読時間Tを導出

まず、決定したパラメータdf、dg、qに対し、非特許文献3に記載の方法で、LLLアルゴリズムを用いた場合の解読時間Tの実測データを実験により求める。ここで、図2に示す解読時間Tの実測データは、1000MIPSの処理能力をもつコンピュータを用いて求めたものであり、解読時間Tの単位は秒である。なお、MIPS (Million Instruction Per Second) とは、コンピュータの処理能力を表す単位であり、1MIPSとは、1秒間に100万命令を実行できる処理能力を表す。本例ではパラメータNとして70から90までの値に対して解読時間が実測可能であったことを示している。

【0088】

(ii) 近似による解読時間評価式の導出

次に、(i)により導出した実測データを用い、解読時間評価式EF

$$EF: \log(T) = A \cdot N + B$$

の定数A、Bを求める。これは、例えば、 $X=N$ 、 $Y=\log(T)$ として、 $Y=A \cdot X+B$ の係数A、Bを最小二乗法により求めれば実現できる。

【0089】

ここで、図2に示す解読時間Tの実測データの場合、定数A、Bは、概ね、 $A=0.093$ 、 $B=-3.8$ となる。

【0090】

基本的には、これにより導出された解読時間評価式EF

$$EF: \log(T) = 0.093N - 3.8$$

を式格納部110に与えてもよいが、以下に詳細を述べる実施の形態1では、解

読時間評価式EFにおける解読時間Tの値を、MIP S y e a r値として扱っている。なお、MIP S y e a rとはコンピュータの処理量を示す単位であり、1 MIP Sの処理能力を持つコンピュータが1年間で処理できる処理量が1 MIP S y e a rである。

【0091】

従って、ここでは、導出された解読時間評価式EFを、非特許文献3に記載の方法で、解読時間Tに、実測データを求めたコンピュータの処理能力値1000 MIP Sを乗じ、1年間の秒数31557600（1年間＝365.25日）で割って、解読時間TがMIP S y e a r値を表すように変形する。

【0092】

すなわち、 $T' = 1000T / 31557600$ とし、前述の解読時間評価式EFに代入することにより、次のように変形した解読時間評価式EFを式格納部110に与える。

【0093】

$$EF: \log(T') = 0.093N - 14.2$$

なお、最小二乗法についてはよく知られた公知の方法であるので、ここでは説明を省略する。

【0094】

（復号エラーが発生しないパラメータの条件式EDの与え方）

次に、条件式EDの与え方について述べる。

【0095】

まず、 $p=3$ とし、 $dg > d$ とする。これは、NTRU暗号のパラメータの典型的な値である。

【0096】

このとき、条件式ED

$$ED: 6d + 2df - 1 < q / 2$$

を予め式格納部110に与えておく。この条件式は、理論的に復号エラーが発生しないパラメータの条件式である。

【0097】

以下に、その理由について説明する。

【0098】

まず、上述したように、多項式 $p \cdot r \times g + f \times m$ の全ての係数が、 $-q/2$ から $q/2$ の範囲に収まっていれば、復号エラーは発生しない。

【0099】

このとき、多項式 $r \times g$ を考えると、多項式の積は、非特許文献2に記載の通り、多項式 a の k 次の係数を $a(k)$ で表すと、

$$\begin{aligned} (r \times g)(k) \\ = r(0) \cdot g(k) + r(1) \cdot g(k-1) + \dots \\ + r(N-1) \cdot g(k - (N-1) \pmod{N}) \end{aligned}$$

である。そして、乱数多項式 r は、 d 個の係数が1であり、かつ d 個の係数が-1であり、かつ他の係数は0となる多項式である。そして、ランダム多項式 g は、 $d \cdot g$ 個の係数が1であり、かつ $d \cdot g$ 個の係数が-1であり、かつ他の係数は0となる多項式である。

【0100】

従って、多項式 $r \times g$ の k 次の係数 $(r \times g)(k)$ の値は、 $d \cdot g > d$ であるので、

$$\begin{aligned} (r \times g)(k) \\ = 1 \cdot g(i_1) + 1 \cdot g(i_2) + \dots + 1 \cdot g(i_d) \\ - 1 \cdot g(j_1) - 1 \cdot g(j_2) - \dots - 1 \cdot g(j_d) \end{aligned}$$

というように、 d 個の $1 \cdot g(i_n)$ という項 ($1 \leq n \leq d$) と d 個の $-1 \cdot g(j_n)$ という項 ($1 \leq n \leq d$) で表される。

【0101】

よって、 $(r \times g)(k)$ は、 $g(i_n)$ が全て1であり ($1 \leq n \leq d$)、かつ $g(j_n)$ が全て-1であるようなとき ($1 \leq n \leq d$) 最大値を取り、その値は、高々 $2d$ である (最小値も、せいぜい $-2d$ である。)。

【0102】

同様に、多項式 $f \times m$ の k 次の係数の値も、その値は高々 $2df-1$ である (最小値も、せいぜい $-2df+1$ である。)。

【0103】

今、 $p=3$ であるので、以上により、多項式 $p \cdot r \times g + f \times m$ の最も大きい係数の値は、高々 $3 \cdot 2d + 2df - 1$ である。そして、最も大きい係数が $q/2$ を超えなければ、多項式 $p \cdot r \times g + f \times m$ の全ての係数は、 $-q/2$ から $q/2$ の範囲に収まっていることになるので、復号エラーは発生しない。

【0104】

従って、以下の条件式 ED が導かれる。

【0105】

$$ED: 6d + 2df - 1 < q/2$$

この条件式を満たせば、以上の議論から復号エラーは理論的に発生しない。

【0106】

<初期安全性決定式 IF >

詳細は後述するが、パラメータ生成装置 1 は、まず、総当り探索の解読に対し安全であるパラメータ df 、 dg 、 d を選ぶために、第 1 のパラメータ生成部 102 において、安全性レベル情報 SLI に応じた十分大きい値であるパラメータ N を選ぶ必要がある。

【0107】

ここでは、そのために、初期安全性決定式 IF の一例として、非特許文献 3 に挙げられている、パラメータ df 、 dg 、 q が、 $df=61$ 、 $dg=20$ 、 $q=128$ の場合の $NTRU$ 暗号における、 LLL アルゴリズムによる解読に必要な解読時間の評価式とし、

$$IF: \log(T) = 0.2002N - 18.884$$

とする。そして、この初期安全性決定式 IF を、式格納部 110 へ与えておく。

【0108】

パラメータ df 、 dg 、 q が、 $df=61$ 、 $dg=20$ 、 $q=128$ の場合の $NTRU$ 暗号における、 LLL アルゴリズムによる解読に必要な解読時間の評価式である、 $\log(T) = 0.2002N - 7.608$ という式を、 T が $MIPS\ Year$ を表すように変換した式である。

【0109】

次に、パラメータ生成装置1の詳細について説明を行う。

【0110】

<パラメータ生成装置1の構成>

パラメータ生成装置1は、図1に示すように、入力部101と、第1のパラメータ生成部102と、第2のパラメータ生成部103と、第3のパラメータ生成部104と、安全性判定部105と、安全性増加部106と、出力部107と、第1のパラメータ変更部108と、第2のパラメータ変更部109と、式格納部110から構成される。以下にそれぞれの構成要素について説明する。

【0111】

(1) 入力部101

入力部101は、外部から安全性レベル情報SLIを受け取り、安全性レベル情報SLIを第1のパラメータ生成部102と第2のパラメータ生成部103と安全性増加部106と第2のパラメータ変更部109に出力する。

【0112】

ここで、安全性レベル情報SLIとは、達成すべき暗号の安全性レベルを表す情報であり、例えば、暗号の安全性が1024ビットRSA暗号に相当する安全性レベルであることを示す情報である。ここでは、一例として、安全性レベル情報SLIは、暗号解読アルゴリズムの処理量とする。ここでは、SLIは (10^{12}) MIPS yearであるとして以降の説明を行う。

【0113】

(2) 第1のパラメータ生成部102

第1のパラメータ生成部102は、入力部101から安全性レベル情報SLIを受け取り、式格納部110から初期安全性決定式IFを読み取り、安全性レベル情報SLIに応じた十分大きい値である、NTRU暗号のパラメータNを選ぶ。そして、選んだパラメータNに対し、パラメータ $p=3$ とし、その他のパラメータ q 、 df 、 dg 、 d の値を仮に0として、パラメータ組 $PS=(N, p, q, df, dg, d)$ を生成して第2のパラメータ生成部103へ出力する。

【0114】

具体的には、パラメータNは、初期安全性決定式IFの値が安全性レベル情報

SLIの表す安全性レベルとなるようにパラメータNを選ぶ。

【0115】

例えば、安全性レベル情報SLIが $(10^{12}) \text{ MIPS year}$ であり、式格納部110に格納されている初期安全性決定式IFが

$$IF: \log(T) = 0.2002N - 18.884$$

であるとき、安全性レベル情報SLIをTに代入した結果

$$IF: \log(10^{12}) = 0.2002N - 18.884$$

を計算することにより、 $N = 233$ を導出する。

【0116】

(3) 第2のパラメータ生成部103

第2のパラメータ生成部103は、第1のパラメータ生成部102もしくは第1のパラメータ変更部108からパラメータ組PSを受け取り、入力部101から安全性レベル情報SLIを受け取る。そして、パラメータ組PSの中のパラメータNに基づき後述する方法によりパラメータ候補集合DSを導出する。そして、後述する方法によりDSの要素数がパラメータdf、dg、dを選ぶのに不十分かどうか（例えば、要素数が3以上かどうか）を判別する。不十分であれば、パラメータ組PSを第1のパラメータ変更部108へ出力する。十分であれば、第2のパラメータ生成部103はパラメータdf、dg、dを、パラメータ候補集合DSから選択し、これらのパラメータdf、dg、dに対し、新たにパラメータ組 $PS = (N, p, q, df, dg, d)$ を生成して第3パラメータ生成部104へ出力する。

【0117】

以下に、パラメータ候補集合DSの導出方法と、パラメータdf、dg、dの選択方法について詳細に説明する。

【0118】

(i) パラメータ候補集合DSの導出方法

安全性レベル情報SLIとパラメータNに対し、

$$(C(N, k) \cdot C(N-k, k))^{(0.5)} \geq SLI$$

を満たす整数 k ($1 \leq k \leq N$) のパラメータ候補集合DSを導出する。ここで、

$C(a, b)$ は a 個の中から b 個を選ぶ組み合わせの数である。

【0119】

これは、例えば、パラメータ N に対し、 $k=1$ から $k=N/2$ まで順に上記の左辺を計算して右辺の安全性レベル情報 SLI と比較し、左辺の値が右辺の安全性レベル情報 SLI 以上の値となるそれぞれの k を、パラメータ候補集合 DS の要素とすることで実現できる。

【0120】

なお、上記の式の左辺は、 $dg=k$ (もしくは $df=k$) としたときには、非特許文献 5 に記載の通り、NTRU 暗号の秘密鍵を総当りで探索する暗号解読の解読時間を示し、 $d=k$ としたときには、非特許文献 5 に記載の通り、NTRU 暗号の平文を総当りで探索する暗号解読の解読時間を示す。すなわち、ここでは、パラメータ候補集合 DS の中からパラメータ df 、 dg 、 d を選べば、平文や秘密鍵を総当りで探索する解読の解読時間が入力部 101 に入力された安全性レベル情報 SLI が表す安全性レベルを達成するように、パラメータ候補集合 DS を導出している。

【0121】

(ii) パラメータ df 、 dg 、 d の選択方法

パラメータ df 、 dg 、 d は、 $dg > d$ となるように、パラメータ候補集合 DS から任意に選択する。ここでは、 $df > dg > d$ となるように、パラメータ候補集合 DS からランダムに選択してそれぞれ df 、 dg 、 d に割り当てることとする。

【0122】

なお、パラメータ候補集合 DS は、十分大きい N に対しては、その要素数がパラメータ df 、 dg 、 d を選ぶのに十分な数となる。実際に、 $SLI=10^{12}$ とすると、 $N=10$ のときには DS の要素は無いが、 $N=30$ のときには $DS = \{8, 9, 10, 11, 12\}$ (8 以上 12 以下の 5 個の整数) となり、 $N=100$ のときには $DS = \{4, 5, 6, \dots, 50\}$ (4 以上 50 以下の 47 個の整数) となる。

【0123】

(4) 第3のパラメータ生成部104

第3のパラメータ生成部104は、第2のパラメータ生成部103からパラメータ組PSを受け取り、式格納部110から復号エラーが発生しないためのパラメータの条件式EDを読み取る。そして、パラメータ組PSの中のパラメータdf、dg、dに対し、条件式EDを満たし、かつ、パラメータqが2の冪となるような最小のqをパラメータqとして選ぶ。そして、選んだパラメータqに対し、新たにパラメータ組PS = (N, p, q, df, dg, d) を生成して安全性判定部105へ出力する。

【0124】

例えば、df = 50、dg = 24、d = 16で、条件式EDが

$$ED: 6d + 2df - 1 < (q/2)$$

のとき、この条件式を解くと $q > 294$ となり、この条件式を満たしかつ $q = 2^i$ (i は自然数) を満たす最小のqは512であるので、パラメータqをq = 512とする。なお、パラメータqを2の冪とするのは、パラメータp (p = 3) とパラメータqを互いに素になるように選ぶためである。pとqが互いに素になることは、非特許文献2に記載の通り、NTRU暗号のパラメータp、qの条件である。

【0125】

(5) 安全性判定部105

安全性判定部105は、第3のパラメータ生成部104もしくは第2のパラメータ変更部109からパラメータ組PSを受け取り、パラメータ組PSの中のパラメータN、p、q、df、dgを持つNTRU暗号の格子強度係数SLを、パラメータdf、dg、qを用いて

$$SL = (4 \cdot \pi \cdot e \cdot |f| \cdot |g| / q)^{(0.5)}$$

により導出する。ここで、 π は円周率、eは自然対数の底、 $|f| = (2df - 1)^{(0.5)}$ 、 $|g| = (2dg)^{(0.5)}$ を表す。

【0126】

そして、安全性判定部105は、式格納部110から格子強度係数GLを読み取り、 $GL \leq SL$ ならば、パラメータ組PSを安全性増加部106へ出力する。

そうでなければ、パラメータ組 P S を第 2 のパラメータ変更部 109 へ出力する。

【0127】

(6) 安全性増加部 106

安全性増加部 106 は、安全性判定部 105 からパラメータ組 P S を受け取り、入力部 101 から安全性レベル情報 S L I を受け取り、式格納部 110 より解読時間評価式 E F を読み取る。そして、パラメータ組 P S 中のパラメータ N と解読時間評価式 E F から N T R U 暗号の解読時間 T を導出する。

【0128】

例えば、 $N = 400$ 、解読時間評価式 E F が、

$$EF: \log(T) = 0.093N - 14.2$$

であるとき、T はおよそ 9.7×10^9 である。

【0129】

そして、安全性増加部 106 は、導出した解読時間 T が、安全性レベル情報 S L I が表す安全性レベルを達成しているかどうかを

$$T \geq S L I$$

を満たすかどうかによって判定する。そして、 $T < S L I$ ならば、解読時間 T が、 $T \geq S L I$ となるようにパラメータ N を増加させ、増加させたパラメータ N に対し、新たにパラメータ組 $PS = (N, p, q, df, dg, d)$ を生成する。

【0130】

これは、例えば、安全性レベル情報 S L I を解読時間評価式 E F の T に代入した結果

$$EF: \log(S L I) = 0.040N - 6.2$$

を計算して N を導出し、パラメータ組 P S を生成すればよい。

【0131】

そして、安全性増加部 106 は、パラメータ組 P S 中のパラメータ N に対し、パラメータ N が素数かどうかを判定する。そして、パラメータ N が素数でなければ、パラメータ N を増加させて素数となるようにして、増加させたパラメータ N に対し、新たにパラメータ組 $PS = (N, p, q, df, dg, d)$ を生成

する。

【0132】

例えば、 $PS = (450, 3, 512, 50, 24, 16)$ の場合、パラメータ N は $N = 450$ であるが素数ではないので、 450 を超える素数のうち最小のものである 451 を新たにパラメータ N の値として、 $PS = (451, 3, 512, 50, 24, 16)$ とする。

【0133】

これは、パラメータ N が合成数だと、NTRU 暗号の安全性が低下することが知られているため、これを避ける目的で行われるものである。なお、素数かどうかを判定する方法は、例えば、非特許文献 1 に記載されており、ここでの説明は省略する。

【0134】

そして、安全性増加部 106 は、パラメータ組 PS を出力部 107 へ出力する。

【0135】

(7) 出力部 107

出力部 107 は、安全性増加部 106 からパラメータ組 PS を受け取って外部へ出力する。

【0136】

(8) 第 1 のパラメータ変更部 108

第 1 のパラメータ変更部 108 は、第 2 のパラメータ生成部 103 もしくは第 2 のパラメータ変更部 109 からパラメータ組 PS を受け取り、パラメータ組 PS 中のパラメータ N を増加させる。ここでは、一例として、 N を 10 増加させるとする。そして、増加させたパラメータ N に対し、新たにパラメータ組 $PS = (N, p, q, df, dg, d)$ を生成して第 2 のパラメータ生成部 103 へ出力する。

【0137】

(9) 第 2 のパラメータ変更部 109

第 2 のパラメータ変更部 109 は、入力部 101 から安全性レベル情報 SLI

を受け取り、安全性判定部 105 からパラメータ組 PS を受け取り、そして、第 2 のパラメータ生成部 103 と同様にして、パラメータ候補集合 DS を生成する。そして、パラメータ組 PS 中のパラメータ d_g とパラメータ候補集合 DS の要素の最大値 M を比較し、 $d_g < M$ であれば、パラメータ d_g を、パラメータ候補集合 DS の要素のうち、より大きい値に変更し、変更したパラメータ d_g に対し、新たにパラメータ組 $PS = (N, p, q, d_f, d_g, d)$ を生成して安全性判定部 105 へ出力する。そうでなければ、パラメータ組 PS を第 1 パラメータ変更部 108 へ出力する。

【0138】

(10) 式格納部 110

式格納部 110 は、図 3 に示すように、予め、格子強度係数 GL 、解読時間評価式 EF 、復号エラーが発生しないパラメータの条件式 ED 、及び初期安全性決定式 IF が与えられている。ここでは、前述のとおり、格子強度係数 GL は、

$$GL = 2.12,$$

解読時間評価式 EF は、

$$EF: \log(T) = 0.93N - 14.2,$$

条件式 ED は、

$$ED: 6d + 2d_f - 1 < (q/2),$$

初期安全性決定式 IF は、

$$IF: \log(T) = 0.2002N - 18.884$$

が、予め与えられているとする。

【0139】

ここで、上記解読時間評価式 EF は、前述したとおり、パラメータ d_f 、 d_g 、 q から計算される格子強度係数の値が、上記格子強度係数 GL の値以上であるとき（この場合は 2.12 以上であるとき）に、LLL アルゴリズムを用いた解読の解読時間 T を、少なく見積もることなく評価できるものである。

【0140】

また、条件式 ED は、前述したとおり、NTRU 暗号において、復号エラーが発生しないためのパラメータ条件を表す式であり、初期安全性決定式 IF は、ま

ず、総当り探索の解読に対し安全であるパラメータ d_f 、 d_g 、 d を選ぶために、第1のパラメータ生成部102において、安全性レベル情報 SLI に応じた十分大きい値であるパラメータ N を選ぶために用いられる式である。

【0141】

<パラメータ生成装置1の動作>

以上に述べたパラメータ生成装置1の動作について、図4、図5に示すフローチャートを用いて説明する。

【0142】

パラメータ生成装置1は、あるパラメータの $NTRU$ 暗号の格子強度係数 GL 、その格子強度係数 GL を持つ $NTRU$ 暗号の解読時間評価式 EF 、及び復号エラーが発生しないパラメータの条件式 ED が予め与えられており、外部より安全性レベル情報 SLI が入力されると、以下の処理を行う。

【0143】

最初に、入力部101は、外部から安全性レベル情報 SLI を受け取り、安全性レベル情報 SLI を第1のパラメータ生成部102と第2のパラメータ生成部103と安全性増加部106に出力する（ステップ $S101$ ）。

【0144】

次に、第1のパラメータ生成部102は、入力部101から安全性レベル情報 SLI を受け取り、式格納部110から初期安全性決定式 IF を読み取り、安全性レベル情報 SLI に応じた十分大きい値である、 $NTRU$ 暗号のパラメータ N を選ぶ（ステップ $S102$ ）。

【0145】

そして、第1のパラメータ生成部102は、選んだパラメータ N に対し、パラメータ $p=3$ とし、その他のパラメータ q 、 d_f 、 d_g 、 d の値を仮に0として、パラメータ組 $PS = (N, p, q, d_f, d_g, d)$ を生成して第2のパラメータ生成部103へ出力する（ステップ $S103$ ）。

【0146】

次に、第2のパラメータ生成部103は、第1のパラメータ生成部102もしくは第1のパラメータ変更部108からパラメータ組 PS を受け取り、入力部1

01から安全性レベル情報SLIを受け取る(ステップS104)。

【0147】

そして、第2のパラメータ生成部103は、パラメータ候補集合DSを生成する(ステップS105)。

【0148】

そして、第2のパラメータ生成部103は、DSの要素数がパラメータdf、dg、dを選ぶのに不十分かどうかを判別し、不十分だったら、処理をステップS107へ移す。そうでなければステップS109へ処理を移す(ステップS106)。

【0149】

そして、第2のパラメータ生成部103は、パラメータ組PSを第1パラメータ変更部108へ出力する。(ステップS107)。

【0150】

次に、第1のパラメータ変更部108は、第2のパラメータ生成部103もしくは第2のパラメータ変更部109からパラメータ組PSを受け取り、パラメータ組PSの中のパラメータNを増加させ、増加させたパラメータNに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成して第2のパラメータ生成部103へ出力する。そして、処理をステップS104へ移す(ステップS108)。

【0151】

そして、第2のパラメータ生成部103は、パラメータ候補集合DSの要素からパラメータdf、dg、dを選び、選んだパラメータdf、dg、dに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成して第3パラメータ生成部104へ出力する(ステップS109)。

【0152】

次に、第3のパラメータ生成部104は、第2のパラメータ生成部103からパラメータ組PSを受け取り、式格納部110から復号エラーが発生しないパラメータの条件式EDを読み取る(ステップS110)。

【0153】

そして、第3のパラメータ生成部104は、パラメータ組PSの中のパラメータdf、dg、dに対し、条件式EDを満たし、かつ、パラメータqが2の冪となるような最小のqをパラメータqとして選び、選んだパラメータqに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成して安全性判定部105へ出力する(ステップS111)。

【0154】

次に、安全性判定部105は、第3のパラメータ生成部104もしくは第2のパラメータ変更部109からパラメータ組PSを受け取り、パラメータ組PSの中のパラメータN、p、q、df、dgをもつNTRU暗号の格子強度係数SLを導出する(ステップS112)。

【0155】

そして、安全性判定部105は、式格納部110から格子強度係数GLを読み取り、 $GL \leq SL$ ならば、ステップS114へ処理を移す。そうでなければ、ステップS123へ処理を移す(ステップS113)。

【0156】

そして、安全性判定部105は、パラメータ組PSを安全性増加部106へ出力する(ステップS114)。

【0157】

次に、安全性増加部106は、安全性判定部105からパラメータ組PSを受け取り、入力部101から安全性レベル情報SLIを受け取り、式格納部110より解読時間評価式EFを読み取る(ステップS115)。

【0158】

そして、安全性増加部106は、パラメータ組PSの中のパラメータNと解読時間評価式EFからNTRU暗号の解読時間Tを導出する(ステップS116)。

。

【0159】

そして、安全性増加部106は、導出した解読時間Tが、 $T < SLI$ ならば、ステップS118へ処理を移す。そうでなければ、ステップS119へ処理を移す(ステップS117)。

【0160】

そして、安全性増加部106は、解読時間 T が $T \geq SLI$ となるようにパラメータ N を増加させ、増加させたパラメータ N に対し、新たにパラメータ組 $PS = (N, p, q, df, dg, d)$ を生成する(ステップS118)。

【0161】

そして、安全性増加部106は、パラメータ N が素数であれば、ステップS121へ処理を移す。そうでなければステップS120へ処理を移す(ステップS119)。

【0162】

そして、安全性増加部106は、パラメータ N を増加させ、増加させたパラメータ N が素数となるようにし、増加させたパラメータ N に対し、新たにパラメータ組 $PS = (N, p, q, df, dg, d)$ を生成する(ステップS120)。

【0163】

そして、安全性増加部106は、パラメータ組 PS を出力部107へ出力する(ステップS121)。

【0164】

次に、出力部107は、安全性増加部106からパラメータ組 PS を受け取り、パラメータ組 PS を外部へ出力して処理を終了する(ステップS122)。

【0165】

次に、第2のパラメータ変更部109は、入力部101から安全性レベル情報 SLI を受け取り、安全性判定部105からパラメータ組 PS を受け取り、パラメータ候補集合 DS を生成する(ステップS123)。

【0166】

そして、第2のパラメータ変更部109は、パラメータ組 PS の中のパラメータ dg とパラメータ候補集合 DS の要素の最大値 M を比較し、 $dg < M$ であれば、処理をステップS125へ移す。そうでなければ、ステップS126へ処理を移す(ステップS124)。

【0167】

そして、第2のパラメータ変更部109は、パラメータ dg を、パラメータ候

補集合DSの要素のうち、より大きい値に変更し、変更したパラメータdgに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成し、パラメータ組PSを安全性判定部105へ出力して、処理をステップS112へ移す(ステップS125)。

【0168】

そして、第2のパラメータ変更部109は、パラメータ組PSを第1のパラメータ変更部108へ出力して、処理をステップS108へ移す(ステップS126)。

【0169】

＜パラメータ生成装置1の動作検証＞

以下に、実施の形態1におけるパラメータ生成装置1の全体の動作について説明する。

【0170】

まず、第1のパラメータ生成部102が、ステップS102において、安全性レベル情報SLIに応じた十分大きい値である、パラメータNを選んでいる。

【0171】

そして、第2のパラメータ生成部103が、ステップS106において、NTRU暗号を総当りで探索する解読に対し、安全性レベル情報SLIの表す安全性レベルを達成するパラメータ候補集合DSを生成して、ステップS109において、このパラメータ候補集合DSの要素から、安全性レベル情報SLIの表す安全性レベルを達成するパラメータdf、dg、dを選んでいる。

【0172】

なお、パラメータ候補集合DSの要素数が不十分な場合は、第1のパラメータ変更部108が、ステップS108において、パラメータNを増加させるようにしている。上述したように、一般に、パラメータNが増加すれば、パラメータ候補集合DSの要素数も大きくなるので、必ずパラメータdf、dg、dは選ぶことができる。

【0173】

そして、第3のパラメータ生成部104が、ステップS111において、復号

エラーが発生しないパラメータの条件式 ED を満たすように、パラメータ q を選ぶことにより、パラメータ組 $PS = (N, p, q, df, dg, d)$ の値が決まる。

【0174】

ここで、パラメータ q の値は、条件式 ED を満たすように選ぶと、同程度のパラメータ df 、 dg 、 d をもつ、非特許文献 2 や非特許文献 3 に記載の NTRU 暗号におけるパラメータ q に比べ、一般に大きくなる。すなわち、格子強度係数 GL の値が小さくなるので、同程度のパラメータ df 、 dg 、 d をもつ非特許文献 2 や非特許文献 3 に記載の NTRU 暗号に比べ、LLL アルゴリズムによる解読に対する安全性レベル（解読時間）が下がる可能性がある。

【0175】

従って、予め格納されている格子強度係数 GL に基づき、安全性判定部 105 が、ステップ S113 において、生成されたパラメータ組 PS をもつ NTRU 暗号の解読時間が、その格子強度係数 GL に基づく解読時間評価式 EF で評価可能かどうかを判断し、そして、評価可能であれば、安全性増加部 106 が、ステップ S118 において、安全性レベル情報 SLI の表す安全性レベルを達成するようにパラメータ N を増加させている。

【0176】

なお、そうでない場合には、第 2 のパラメータ変更部 109 が、ステップ S125 において、パラメータ dg をより大きい値にすることにより、そのパラメータをもつ NTRU 暗号の格子強度係数の値を大きくして、解読時間評価式 EF で評価できるようにするか、それに対応できない場合は、第 1 のパラメータ変更部 108 が、ステップ S108 で、パラメータ N を増加させ、そしてステップ S109 以降で、もう一度パラメータ df 、 dg 、 d 、 q の生成を行うようにしている。

【0177】

今、パラメータ N を大きくとれば、一般にパラメータ候補集合 DS は大きい要素をもつようになる。よって、ステップ S109 で、パラメータ df 、 dg 、 d をもう一度選び直すときには、 df 、 d の値を変えずに、 dg のみ値を大きくと

ることができる。そして、 dg の値は、復号エラー発生 の条件式には関与しないので、復号エラーが発生しないことを保証したまま、格子強度係数 GL の値を大きくして、解読時間評価式 EF で評価できるようにすることが可能となる。

【0178】

以上により、高々有限回の繰り返し回数で、総当りの探索による解読とLLLアルゴリズムによる解読に対し、入力された安全性レベル情報 SLI の表す安全性を達成し、かつ、復号エラーが発生しないNTRU暗号のパラメータ PS を生成することができる。

【0179】

<実施の形態1における効果>

従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータを生成するための条件が知られておらず、そのようなNTRU暗号のパラメータを生成できなかった。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができなかった。

【0180】

しかしながら、このパラメータ生成装置は、上述したように、理論的に復号エラーが発生しないようにパラメータ q を決定し、また入力された安全性レベルを達成するようにパラメータ N を決定するようにしたので、安全かつ理論的に復号エラーが発生しないNTRU暗号のパラメータを生成できるようになった。

【0181】

(実施の形態2)

本発明に係る実施の形態2としてのパラメータ変換装置2について、実施の形態1との差異点を中心に説明する。

【0182】

<パラメータ変換装置2の概要>

最初に、図6を用いて本実施の形態の概要を説明する。

【0183】

このパラメータ変換装置2は、実施の形態1におけるパラメータ生成装置1を變形した構成したパラメータ変換装置であり、NTRU暗号のパラメータ組 IP

Sとを入力としたとき、パラメータ組IPSを、総当りの探索による解読とLLアルゴリズムによる解読に対し、入力された安全性レベル情報SLIを達成し、かつ復号エラーが発生しないNTRU暗号のパラメータ組PSへ変換して出力する点が、パラメータ生成装置1と異なる。

【0184】

なお、実施の形態1におけるパラメータ生成装置1と同様にして、あるパラメータのNTRU暗号の格子強度係数GL、その格子強度係数GLを持つNTRU暗号の解読時間評価式EF、及び復号エラーが発生しないパラメータの条件式EDが予め与えられている。

【0185】

<パラメータ変換装置2の構成>

パラメータ変換装置2は、図6に示すように、入力部101bと、第2のパラメータ生成部103bと、第3のパラメータ生成部104bと、安全性判定部105と、安全性増加部106と、出力部107と、第1のパラメータ変更部108と、第2のパラメータ変更部109と、式格納部110から構成される。

【0186】

このパラメータ変換装置2は、入力部101bが異なることと、第1のパラメータ生成部が存在しないことと、第2のパラメータ生成部103bの入出力が異なることと、及び第3のパラメータ生成部104bの入出力が異なることとが、実施の形態1におけるパラメータ生成装置1と異なる。

【0187】

ここでは、パラメータ生成装置1との差異点を中心に説明を行う。

【0188】

(1) 入力部101b

入力部101bは、外部から安全性レベル情報SLIとNTRU暗号のパラメータ組IPSを受け取り、安全性レベル情報SLIを第2のパラメータ生成部103bと安全性増加部106と第2のパラメータ変更部109に出力し、そして、パラメータ組IPSをパラメータ組PSとして第3のパラメータ生成部104bへ出力する。

【0189】

(2) 第2のパラメータ生成部103b

第2のパラメータ生成部103bは、第1のパラメータ変更部108からパラメータ組PSを受け取り、入力部101bから安全性レベル情報SLIを受け取る。そして、第2のパラメータ生成部103と同様にして、パラメータ候補集合DSを生成する。そして、第2のパラメータ生成部103と同様にして、DSの要素数がパラメータdf、dg、dを選ぶのに不十分かどうか（例えば、要素数が3以上かどうか）を判別し、不十分だったら、パラメータ組PSを第1パラメータ変更部108へ出力する。そうでなければ、パラメータdf、dg、dを、パラメータ候補集合DSから選び、選んだパラメータdf、dg、dに対し、新たにパラメータ組PS = (N, p, q, df, dg, d) を生成してパラメータ組PSを第3パラメータ生成部104bへ出力する。

【0190】

(3) 第3のパラメータ生成部104b

第3のパラメータ生成部104bは、入力部101bもしくは第2のパラメータ生成部103bからパラメータ組PSを受け取り、式格納部110から復号エラーが発生しないパラメータの条件式EDを読み取る。そして、第3のパラメータ生成部104と同様にして、パラメータ組PSの中のパラメータdf、dg、dに対し、条件式EDを満たし、かつ、パラメータqが2の冪となるような最小のqをパラメータqとして選ぶ。そして、選んだパラメータqに対し、新たにパラメータ組PS = (N, p, q, df, dg, d) を生成し、パラメータ組PSを安全性判定部105へ出力する。

【0191】

<パラメータ変換装置2の動作>

以上に述べたパラメータ変換装置2の動作について、図7、図8に示すフローチャートを用いて説明する。

【0192】

パラメータ変換装置2は、実施の形態1のパラメータ生成装置1と同様にして、あるパラメータのNTRU暗号の格子強度係数GL、その格子強度係数GLを

持つNTRU暗号の解読時間評価式EF、及び復号エラーが発生しないパラメータの条件式EDが予め与えられており、外部より安全性レベル情報SLI及びNTRU暗号のパラメータ組IPSが入力されると、以下の処理を行う。

【0193】

最初に、入力部101bは、外部から安全性レベル情報SLIとNTRU暗号のパラメータ組IPSを受け取り、安全性レベル情報SLIを第2のパラメータ生成部103bと安全性増加部106と第2のパラメータ変更部109に出力し、パラメータ組IPSをパラメータ組PSとして第3のパラメータ生成部104bへ出力し、処理をステップS210へ移す（ステップS201）。

【0194】

次に、第2のパラメータ生成部103bは、第1のパラメータ変更部108からパラメータ組PSを受け取り、入力部101から安全性レベル情報SLIを受け取る（ステップS204）。

【0195】

そして、第2のパラメータ生成部103bは、パラメータ候補集合DSを生成する（ステップS205）。

【0196】

そして、第2のパラメータ生成部103bは、DSの要素数がパラメータdf、dg、dを選ぶのに不十分かどうかを判別し、不十分だったら、処理をステップS207へ移す。そうでなければステップS209へ処理を移す（ステップS206）。

【0197】

そして、第2のパラメータ生成部103bは、パラメータ組PSを第1パラメータ変更部108へ出力する。（ステップS207）。

【0198】

次に、第1のパラメータ変更部108は、第2のパラメータ生成部103bもしくは第2のパラメータ変更部109からパラメータ組PSを受け取り、パラメータ組PSの中のパラメータNを増加させ、増加させたパラメータNに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成して第2のパラ

メータ生成部103bへ出力する。そして、処理をステップS204へ移す（ステップS208）。

【0199】

そして、第2のパラメータ生成部103bは、パラメータ候補集合DSの要素からパラメータdf、dg、dを選び、選んだパラメータdf、dg、dに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成して第3パラメータ生成部104bへ出力する（ステップS209）。

【0200】

次に、第3のパラメータ生成部104bは、入力部101bからパラメータ組PSを受け取り、式格納部110から復号エラーが発生しないパラメータの条件式EDを読み取る（ステップS210）。

【0201】

そして、第3のパラメータ生成部104bは、パラメータ組PSの中のパラメータdf、dg、dに対し、条件式EDを満たし、かつ、パラメータqが2の冪となるような最小のqをパラメータqとして選び、選んだパラメータqに対し、新たにパラメータ組PS=(N, p, q, df, dg, d)を生成して安全性判定部105へ出力する（ステップS211）。

【0202】

次に、安全性判定部105は、第3のパラメータ生成部104bもしくは第2のパラメータ変更部109からパラメータ組PSを受け取り、パラメータ組PSの中のパラメータN、p、q、df、dgをもつNTRU暗号の格子強度係数SLを導出する（ステップS212）。

【0203】

そして、安全性判定部105は、式格納部110から格子強度係数GLを読み取り、 $GL \leq SL$ ならば、ステップS214へ処理を移す。そうでなければ、ステップS223へ処理を移す（ステップS213）。

【0204】

そして、安全性判定部105は、パラメータ組PSを安全性増加部106へ出力する（ステップS214）。

【0205】

次に、安全性増加部106は、安全性判定部105からパラメータ組PSを受け取り、入力部101bから安全性レベル情報SLIを受け取り、式格納部110より解読時間評価式EFを読み取る（ステップS215）。

【0206】

そして、安全性増加部106は、パラメータ組PSの中のパラメータNと解読時間評価式EFからNTRU暗号の解読時間Tを導出する（ステップS216）。

【0207】

そして、安全性増加部106は、導出した解読時間Tが、 $T < SLI$ ならば、ステップS218へ処理を移す。そうでなければ、ステップS219へ処理を移す（ステップS217）。

【0208】

そして、安全性増加部106は、解読時間Tが $T \geq SLI$ となるようにパラメータNを増加させ、増加させたパラメータNに対し、新たにパラメータ組PS = (N, p, q, df, dg, d) を生成する（ステップS218）。

【0209】

そして、安全性増加部106は、パラメータNが素数であれば、ステップS221へ処理を移す。そうでなければステップS220へ処理を移す（ステップS219）。

【0210】

そして、安全性増加部106は、パラメータNを増加させ、増加させたパラメータNが素数となるようにし、増加させたパラメータNに対し、新たにパラメータ組PS = (N, p, q, df, dg, d) を生成する（ステップS220）。

【0211】

そして、安全性増加部106は、パラメータ組PSを出力部107へ出力する（ステップS221）。

【0212】

次に、出力部107は、安全性増加部106からパラメータ組PSを受け取り

、パラメータ組P Sを外部へ出力して処理を終了する（ステップS 2 2 2）。

【0 2 1 3】

次に、第2のパラメータ変更部1 0 9は、入力部1 0 1 bから安全性レベル情報S L Iを受け取り、安全性判定部1 0 5からパラメータ組P Sを受け取り、パラメータ候補集合D Sを生成する（ステップS 2 2 3）。

【0 2 1 4】

そして、第2のパラメータ変更部1 0 9は、パラメータ組P Sの中のパラメータd gとパラメータ候補集合D Sの要素の最大値Mを比較し、 $d g < M$ であれば、処理をステップS 2 2 5へ移す。そうでなければ、ステップS 2 2 6へ処理を移す（ステップS 2 2 4）。

【0 2 1 5】

そして、第2のパラメータ変更部1 0 9は、パラメータd gを、パラメータ候補集合D Sの要素のうち、より大きい値に変更し、変更したパラメータd gに対し、新たにパラメータ組 $P S = (N, p, q, d f, d g, d)$ を生成し、パラメータ組P Sを安全性判定部1 0 5へ出力して、処理をステップS 2 1 2へ移す（ステップS 2 2 5）。

【0 2 1 6】

そして、第2のパラメータ変更部1 0 9は、パラメータ組P Sを第1のパラメータ変更部1 0 8へ出力して、処理をステップS 2 0 8へ移す（ステップS 2 2 6）。

【0 2 1 7】

＜パラメータ変換装置2の動作検証＞

以下に、実施の形態2におけるパラメータ変換装置2の全体の動作について説明する。

【0 2 1 8】

まず、入力部1 0 1 bが、ステップS 2 0 1において、入力されたN T R U暗号のパラメータ組I P Sをパラメータ組P Sとして第3のパラメータ生成部1 0 4 bに出力している。

【0 2 1 9】

そして、第2のパラメータ生成部103bは、実施の形態1と同様にして、NTRU暗号を総当りで探索する解読に対し、安全性レベル情報SLIの表す安全性レベルを達成するパラメータ候補集合DSを生成する（ステップS205）。

【0220】

そして、第3のパラメータ生成部104が、ステップS211において、復号エラーが発生しないパラメータの条件式EDを満たすように、パラメータqを選ぶことにより、パラメータ組PS = (N, p, q, df, dg, d)の値が決まる。

【0221】

ここで、実施の形態1と同様に、パラメータqの値を、条件式EDを満たすように選ぶと、LLLアルゴリズムによる解読に対する安全性レベル（解読時間）が下がる可能性があるので、予め格納されている格子強度係数GLに基づき、安全性判定部105が、ステップS213において、生成されたパラメータ組PSをもつNTRU暗号の解読時間が、その格子強度係数GLに基づく解読時間評価式EFで評価可能かどうかを判断し、そして、評価可能であれば、安全性増加部106が、ステップS218において、安全性レベル情報SLIの表す安全性レベルを達成するようにパラメータNを増加させている。

【0222】

なお、そうでない場合には、第2のパラメータ変更部109が、ステップS225において、パラメータdgをより大きい値にすることにより、そのパラメータをもつNTRU暗号の格子強度係数の値を大きくして、解読時間評価式EFで評価できるようにするか、それに対応できない場合は、第1のパラメータ変更部108が、ステップS208で、パラメータNを増加させ、そしてステップS209以降で、もう一度パラメータdf、dg、d、qの生成を行うようにしている。

【0223】

今、パラメータNを大きくとれば、一般にパラメータ候補集合DSは大きい要素をもつようになる。よって、ステップS209で、パラメータdf、dg、dをもう一度選び直すときには、df、dの値を変えずに、dgのみ値を大きくと

ることができる。そして、 dg の値は、復号エラー発生 の条件式には関与しないので、復号エラーが発生しないことを保証したまま、安全強度指標 GL の値を大きくして、解読時間評価式 EF で評価できるようにすることが可能となる。

【0224】

以上により、高々有限回の繰り返し回数で、入力された $NTRU$ 暗号のパラメータ IPS を、総当りの探索による解読と LLL アルゴリズムによる解読に対し、入力された安全性レベル情報 SLI の表す安全性レベルを達成し、かつ、復号エラーが発生しない $NTRU$ 暗号のパラメータ PS に変換することができる。

【0225】

<実施の形態2における効果>

従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しない $NTRU$ 暗号のパラメータを生成するための条件が知られておらず、そのような $NTRU$ 暗号のパラメータを生成できなかった。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができなかった。

【0226】

しかしながら、このパラメータ変換装置は、上述したように、入力された $NTRU$ 暗号のパラメータに対し、理論的に復号エラーが発生しないようにパラメータ q を決定し、また入力された安全性レベルを達成するようにパラメータ N を決定するようにしたので、安全でかつ理論的に復号エラーが発生しない $NTRU$ 暗号のパラメータに変換できるようになった。

【0227】

(実施の形態3)

本発明に係る実施の形態3としての暗号システム3について説明する。

【0228】

<暗号システム3の構成>

この暗号システム3は、図11に示すように、暗号装置31、復号装置32、及び通信路33から構成され、実施の形態1におけるパラメータ生成装置1あるいは実施の形態2におけるパラメータ変換装置2によって生成された、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しない $NTRU$ 暗号の

パラメータを利用して、暗号化通信を行うシステムである。

【0229】

<暗号装置 31 の構成>

暗号装置 31 は、図 12 に示すように、パラメータ記憶部 311、公開鍵記憶部 312、暗号化部 313 から構成される。

【0230】

(1) パラメータ記憶部 311

パラメータ記憶部 311 は、実施の形態 1 におけるパラメータ生成装置 1 あるいは実施の形態 2 におけるパラメータ変換装置 2 によって生成された NTRU 暗号のパラメータである、パラメータ N 、パラメータ p 、パラメータ q 、パラメータ df 、パラメータ dg 、パラメータ d を、予め記憶している。

【0231】

(2) 公開鍵記憶部 312

公開鍵記憶部 312 は、予め復号装置 32 の公開鍵多項式 h を取得し、記憶している。

【0232】

この公開鍵多項式 h は、パラメータ N に対し、 $N-1$ 次元以下の多項式で表される多項式である。

【0233】

(3) 暗号化部 313

暗号化部 313 は、パラメータ記憶部 311 からパラメータ N 、パラメータ p 、パラメータ q 、パラメータ d を受け取り、公開鍵記憶部 312 から、公開鍵多項式 h を受け取り、外部から、パラメータ N に対し、 $N-1$ 次元以下の多項式で表される平文多項式 m を受け取る。

【0234】

そして、パラメータ N 、パラメータ d を用いて、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつ他の係数は 0 となるように、 $N-1$ 次元の乱数多項式 r をランダムに選ぶ。

【0235】

そして、平文多項式 m に対し、乱数多項式 r 、公開鍵多項式 h 、パラメータ N 、パラメータ p 、パラメータ q を用いて、NTRU 暗号の暗号化処理を行い、暗号文多項式 c を計算する。

【0236】

この暗号文多項式 c の演算方法の詳細は、非特許文献 2 に記載されているため、ここでは説明を省略する。そして、生成した暗号文多項式 c を通信路 33 を介して復号装置 32 へ送信する。

【0237】

＜復号装置 32 の構成＞

復号装置 32 は、図 13 に示すように、パラメータ記憶部 321、鍵生成部 322、秘密鍵記憶部 323、復号化部 324 から構成される。

【0238】

(1) パラメータ記憶部 321

パラメータ記憶部 321 は、暗号装置 31 のパラメータ記憶部 311 が記憶する NTRU 暗号のパラメータと同じ NTRU 暗号のパラメータを記憶している。

【0239】

すなわち、パラメータ記憶部 311 が記憶するものと同じパラメータ N 、パラメータ p 、パラメータ q 、パラメータ d_f 、パラメータ d_g 、パラメータ d を、予め記憶している。

【0240】

(2) 鍵生成部 322

鍵生成部 322 は、パラメータ記憶部 321 からパラメータ N 、パラメータ p 、パラメータ q 、パラメータ d_f 、パラメータ d_g を受け取り、パラメータ N 、パラメータ p 、パラメータ q 、パラメータ d_f 、パラメータ d_g を用いて、 $N-1$ 次元以下の多項式で表される秘密鍵多項式 f 、及び公開鍵多項式 h を生成する。なお、この秘密鍵多項式 f 及び公開鍵多項式 h の生成方法は、非特許文献 2 に記載されているため、ここでは説明を省略する。

【0241】

そして、公開鍵多項式 h を公開して暗号装置 31 が取得できるようにし、秘密

鍵多項式 f を秘密鍵記憶部 323 に記憶する。

【0242】

(3) 秘密鍵記憶部 323

秘密鍵記憶部 323 は、予め復号装置 32 の秘密鍵多項式 f を記憶している。

【0243】

この秘密鍵多項式 f は、パラメータ N に対し、 $N-1$ 次元以下の多項式で表される多項式である。

【0244】

(4) 復号化部 324

復号化部 324 は、パラメータ記憶部 321 から、パラメータ N 、パラメータ p 、パラメータ q を受け取り、秘密鍵記憶部 323 から、秘密鍵多項式 f を受け取り、通信路 33 を介して暗号装置 31 から暗号文多項式 c を受け取る。

【0245】

そして、暗号文多項式 c に対し、秘密鍵多項式 f 、パラメータ N 、パラメータ p 、パラメータ q を用いて、NTRU 暗号の復号化処理を行い、復号文多項式 m' を計算する。この NTRU 暗号の復号化処理の詳細は、非特許文献 2 に記載されているため、ここでは説明を省略する。

【0246】

そして、生成した復号文多項式 m' を外部へ出力する。

【0247】

<暗号システム 3 の動作>

以上に述べた暗号システム 3 の動作について説明する。

【0248】

暗号システム 3 は、実施の形態 1 におけるパラメータ生成装置 1 あるいは実施の形態 2 におけるパラメータ変換装置 2 によって生成された、NTRU 暗号のパラメータに対し、少なくとも、パラメータ N 、パラメータ p 、パラメータ q 、パラメータ d を暗号装置 31 のパラメータ記憶部 311 に記憶しており、少なくともパラメータ N 、パラメータ p 、パラメータ q 、パラメータ d_f 、パラメータ d_g を復号装置 32 のパラメータ記憶部 321 に記憶している（ステップ S301

)。

【0249】

そして、復号装置 32 の鍵生成部 322 は、パラメータ記憶部 321 からパラメータ N 、パラメータ p 、パラメータ q 、パラメータ d_f 、パラメータ d_g を受け取り、秘密鍵多項式 f 、及び公開鍵多項式 h を生成して、公開鍵多項式 h を公開して暗号装置 31 が取得できるようにし、秘密鍵多項式 f を秘密鍵記憶部 323 に記憶する (ステップ S302)。

【0250】

そして、暗号装置 31 の公開鍵記憶部 312 は、復号装置 32 の公開鍵多項式 h を取得し記憶する (ステップ S303)。

【0251】

そして、暗号装置 31 の暗号化部 313 は、パラメータ記憶部 311 からパラメータ N 、パラメータ p 、パラメータ q 、パラメータ d を受け取り、公開鍵記憶部 312 から、公開鍵多項式 h を受け取り、外部から、パラメータ N に対し、 $N-1$ 次元以下の多項式で表される平文多項式 m を受け取る (ステップ S304)。

【0252】

そして、暗号装置 31 の暗号化部 313 は、パラメータ N 、パラメータ d を用いて、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつ他の係数は 0 となるように、 $N-1$ 次元の乱数多項式 r をランダムに選び、平文多項式 m に対し、乱数多項式 r 、公開鍵多項式 h 、パラメータ N 、パラメータ p 、パラメータ q を用いて、NTRU 暗号の暗号化処理を行い、暗号文多項式 c を計算する (ステップ S305)。

【0253】

そして、暗号装置 31 の暗号化部 313 は、暗号文多項式 c を通信路 33 を介して復号装置 32 へ送信する (ステップ S306)。

【0254】

そして、復号装置 32 の復号化部 324 は、パラメータ記憶部 321 から、パラメータ N 、パラメータ p 、パラメータ q を受け取り、秘密鍵記憶部 323 から

、秘密鍵多項式 f を受け取り、通信路 33 を介して暗号装置 31 から暗号文多項式 c を受け取る（ステップ S307）。

【0255】

そして、復号装置 32 の復号化部 324 は、暗号文多項式 c に対し、秘密鍵多項式 f 、パラメータ N 、パラメータ p 、パラメータ q を用いて、NTRU 暗号の復号化処理を行い、復号文多項式 m' を計算する（ステップ S308）。

【0256】

そして、復号装置 32 の復号化部 324 は、復号文多項式 m' を外部へ出力して処理を終了する（ステップ S309）。

【0257】

<暗号システム 3 の動作検証>

まず、復号装置 32 は、ステップ S302 において、実施の形態 1 におけるパラメータ生成装置 1 あるいは実施の形態 2 におけるパラメータ変換装置によって生成された NTRU 暗号のパラメータを用いて、秘密鍵多項式 f 、公開鍵多項式 h を生成している。

【0258】

そして、暗号装置 31 が、ステップ S305 において、実施の形態 1 におけるパラメータ生成装置 1 あるいは実施の形態 2 におけるパラメータ変換装置によって生成された NTRU 暗号のパラメータを用いて、平文多項式 m を暗号化している。

【0259】

以上により、実施の形態 1 におけるパラメータ生成装置 1 あるいは実施の形態 2 におけるパラメータ変換装置 2 によって生成されたパラメータを用いて、秘密鍵多項式 f 、公開鍵多項式 h を生成して暗号化を行っているため、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないことがいえる。

【0260】

<実施の形態 3 における効果>

従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しない NTRU 暗号のパラメータを生成するための条件が知られておらず

、そのようなNTRU暗号のパラメータを生成できなかった。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができなかった。

【0261】

しかしながら、この暗号システムは、上述したように、実施の形態1におけるパラメータ生成装置1あるいは実施の形態2におけるパラメータ変換装置2によって生成されたパラメータを用いて、秘密鍵多項式 f 、公開鍵多項式 h を生成して暗号化をおこなっているため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるようになった。

【0262】

<変形例>

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0263】

(1) 式格納部110に格納される格子強度係数 GL 及び解読時間評価式 EF は、図10に示す通り複数の組が格納され、安全性判定部105が $GL \leq SL$ を満たす格子強度係数 GL と解読時間評価式 EF の組を読み取ってもよい。

【0264】

また、式格納部110に格納される格子強度係数 GL 及び解読時間評価式 EF は、後で変更できるようにしてもよい。

【0265】

(2) 第1のパラメータ生成部102におけるパラメータ N の選択方法は、この方法に限定されず、 N が十分大きくとれる方法であれば任意の方法でよい。例えば、 $F(x) = 10 \cdot \log(x)$ 等の単調増加関数 F に対し、 $N = F(SLI)$ によって選択してもよい。また、例えば、パラメータ N は固定値であってもよい。

【0266】

(3) 第2のパラメータ生成部103におけるパラメータ df 、 dg 、 d の選択方法は、この方法に限定されず、総当りで探索する解読に対し、秘密鍵の安全

性レベルと平文の安全性レベルが安全性レベル情報 S L I が表す安全性レベルを達成し、かつ $d_g > d$ となるように選択すれば、どのような方法でもよい。

【0267】

(4) また、パラメータ組 P S 中のパラメータ q 、 d_f 、 d_g 、 d は、第2のパラメータ生成部 103 が上述の方法でパラメータ d_f 、 d_g 、 d を選択し、第3のパラメータ生成部 104 が条件式 E D にパラメータ d_f 、 d_g 、 d の値を適用してパラメータ q の値を決定することにより生成する以外にも、パラメータ q が外部から予め与えられており、条件式 E D とパラメータ q の値から導出される関係式に基づいて、 $d_g > d$ となるようにパラメータ d_f 、 d_g 、 d を選択することにより生成してもよい。

【0268】

具体的には、例えばパラメータ q として $q = 256$ が外部から予め与えられている場合、条件式 E D とパラメータ q の値から、

$$6d + 2d_f - 1 < 128$$

という関係式を満たし、かつ $d_g > d$ となるようにパラメータ d_f 、 d_g 、 d を選び、パラメータ組 P S 中のパラメータ q 、 d_f 、 d_g 、 d を生成してもよい。

【0269】

なお、この場合、パラメータ d_f 、 d_g 、 d は、総当りで探索する解読に対し、秘密鍵や平文の解読時間が安全性レベル情報 S L I が表す安全性レベルを達成していない可能性がある。そのため、安全性増加部 106 が、上述のように、L L L アルゴリズムによる解読時間 T が安全性レベル情報 S L I を達成するようにパラメータ N を増加させた後、第2のパラメータ生成部 103 の構成において説明した秘密鍵や平文を総当りで探索する暗号解読の解読時間が、安全性レベル情報 S L I が表す安全性レベルを達成するようにパラメータ N を増加してもよい。

【0270】

また、秘密鍵や平文を総当りで探索する暗号解読の解読時間が、安全性レベル情報 S L I が表す安全性レベルを達成するようにパラメータ N を増加させた後、L L L アルゴリズムによる解読時間 T が安全性レベル情報 S L I を達成するよう

にパラメータ N を増加させてもよい。

【0271】

(5) 第3のパラメータ生成部104におけるパラメータ q の選択方法は、この方法に限定されず、条件式 ED を満たし、かつパラメータ p と互いに素になるように選択すれば、どのような方法でもよい。

【0272】

(6) 第1のパラメータ生成部102が生成するパラメータ p 、及びパラメータ変換装置2が扱うパラメータ組 IPS 、 PS 中のパラメータ p は、 $p=3$ に限定されず、他のものでもよい。

【0273】

例えば、ある非負整数 k に対して $p=k$ とした場合、式格納部110に格納される条件式 ED を

$$ED: 2 \cdot k \cdot d + 2df - 1 < q/2$$

とすれば、同様の効果が得られる。

【0274】

(7) 上記変形例(6)に関し、さらに、ある多項式 b に対して $p=b$ としてもよい。例えば、 $p=(X+2)$ とした場合、

この場合、式格納部110に格納される条件式 ED を

$$ED: 6d + 2df - 1 < q/2$$

とすれば、同様の効果が得られる。

【0275】

何故ならば、上述した通り、多項式 $p \times r \times g + f \times m$ の全ての係数が、 $-q/2$ から $q/2$ の範囲に収まっていれば、復号エラーは発生しないのであった。

【0276】

このとき、多項式 $r \times g$ を考えると、その係数の最大値は、高々 $2d$ であった(最小値も、せいぜい $-2d$ 。)。

【0277】

今、 $p=(X+2)$ なので、多項式 a の k 次の係数を $a(k)$ で表すと、

$$p(0)=2, p(1)=1, p(i)=0 \quad (i>1)$$

であるので、

$$\begin{aligned}
 & (p \times (r \times g)) (k) \\
 &= p(0) \cdot (r \times g)(k) + p(1) \cdot (r \times g)(k-1) + \\
 & \quad \dots + p(N-1) \cdot (r \times g)(k - (N-1) \pmod{N}) \\
 &= (r \times g)(k) + 2 \cdot (r \times g)(k-1)
 \end{aligned}$$

である。

【0278】

よって、多項式 $p \times r \times g$ を考えると、その係数の最大値は、 $3 \cdot 2d$ である。一方、多項式 $f \times m$ の係数の値は、その値が高々 $2df-1$ であった（最小値も、せいぜい $-2df+1$ 。）。

【0279】

従って、実施の形態で説明したのと同様にして、多項式 $p \times r \times g + f \times m$ の最も大きい係数の値は、高々 $3 \cdot 2d + 2df - 1$ であることが導くことができ、ここから、復号エラーが理論的に発しない条件式 ED として、

$$ED: 6d + 2df - 1 < q/2$$

を導くことができる。

【0280】

なお、多項式 b は $b = (X+2)$ に限定されないことはもちろんである。その場合、上述の処理を行えば、条件式 ED を導くことができ、同様の効果が得られる。

【0281】

(8) なお、パラメータ変換装置2において、パラメータ組 IPS を外部より入力する以外にも、入力部101bが、安全性レベル情報 SLI が表す安全性レベルを達成する、パラメータ組 IPS のリストを保持して、外部よりの入力安全性レベル情報 SLI だけにしてもよい。すなわち、入力部101bが、図9に示すようなパラメータ組 IPS のリストを保持しており、外部から安全性レベル情報 SLI が入力されると、この SLI に関連付けられたパラメータ組 IPS をパラメータ組 PS として第3のパラメータ生成部105へ出力してもよい。

【0282】

(9) なお、非特許文献4には、Zero-Run Latticeを用いる解読により、LLLアルゴリズムの解読時間が減少する可能性があることが記載されているが、解読時間評価式EFは、このZero-Run Latticeを用いた解読を考慮した、LLLアルゴリズムの解読時間としてもよい。

【0283】

(10) なお、暗号システム3において、秘密鍵多項式f及び公開鍵多項式hは、復号装置32の鍵生成部322で生成される以外にも、これらが例えば鍵管理サーバ等の復号装置32の外部で生成されて、秘密鍵多項式fが、外部から秘密鍵記憶部323へ入力され、公開鍵多項式hが、外部から公開鍵記憶部312へ入力されるようにしてもよい。

【0284】

(11) なお、暗号システム3において、暗号システム3は、さらに実施の形態1におけるパラメータ生成装置1、あるいは実施の形態2におけるパラメータ変換装置2を備え、パラメータ生成装置1あるいはパラメータ変換装置2が出力したNTRU暗号のパラメータが、パラメータ記憶部311、321に入力されるようにしてもよい。

【0285】

(12) 変形例(11)に関し、暗号システム3において、暗号装置31が、さらに、実施の形態1におけるパラメータ生成装置1あるいはパラメータ変換装置2の構成要素を含み、暗号装置31がNTRU暗号のパラメータを生成し、生成したNTRU暗号のパラメータが、パラメータ記憶部311に入力され、通信路33を介して復号装置32へ送信され、復号装置32で受信されたこのNTRU暗号のパラメータがパラメータ記憶部321に入力されるようにしてもよい。

【0286】

(13) パラメータ記憶部311に記憶されるNTRU暗号パラメータは、パラメータN、p、q、df、dg、dのうち、少なくとも、パラメータN、パラメータp、パラメータq、パラメータdを含めば、どのようなものでもよい。また、パラメータ記憶部321に記憶されるNTRU暗号パラメータは、少なくとも、パラメータN、パラメータp、パラメータq、パラメータdf、パラメータ

dgを含めば、どのようなものでもよい。

【0287】

(14) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0288】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、CD-ROM、DVD-ROM、DVD-RAM等、に記録したものとしてもよい。

【0289】

(15) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0290】

【発明の効果】

以上に説明したように、本発明は、従来技術における問題点を鑑みて行われたもので、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータを生成するパラメータ生成装置を構成することができるようになった。

【0291】

また、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、入力されたNTRU暗号のパラメータに対し、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータに変換するパラメータ変換装置を構成できるようになった。

【0292】

さらに、これらのパラメータ装置もしくはパラメータ変換装置により生成されたパラメータを用いて、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができる、暗号システム、暗号装置及び復号装置を構成できるようになった。

【0293】

以上により、従来技術では達成できなかったパラメータ生成装置、パラメータ変換装置、暗号システム、暗号装置、及び復号装置を提供することができ、その価値は大きい。

【図面の簡単な説明】

【図1】

本発明の実施の形態1におけるパラメータ生成装置1の構成を示す図

【図2】

パラメータNにおける解読時間Tの実測データを示す図

【図3】

本発明の実施の形態1における式格納部110の構成を示す図

【図4】

本発明の実施の形態1におけるパラメータ生成装置1の処理の前半部を表す図

【図5】

本発明の実施の形態1におけるパラメータ生成装置1の処理の後半部を表す図

【図6】

本発明の実施の形態2におけるパラメータ変換装置2の構成を示す図

【図7】

本発明の実施の形態2におけるパラメータ変換装置2の処理の前半部を示す図

【図8】

本発明の実施の形態2におけるパラメータ変換装置2の処理の後半部を示す図

【図9】

安全性レベル情報とその安全性レベルを達成するNTRU暗号のパラメータ組を示す図

【図10】

本発明の変形例(1)における式格納部110の構成を示す図

【図11】

本発明の実施の形態3における暗号システム3の構成を示す図

【図12】

本発明の実施の形態 3 における暗号装置 31 の構成を示す図

【図 13】

本発明の実施の形態 3 における復号装置 32 の構成を示す図

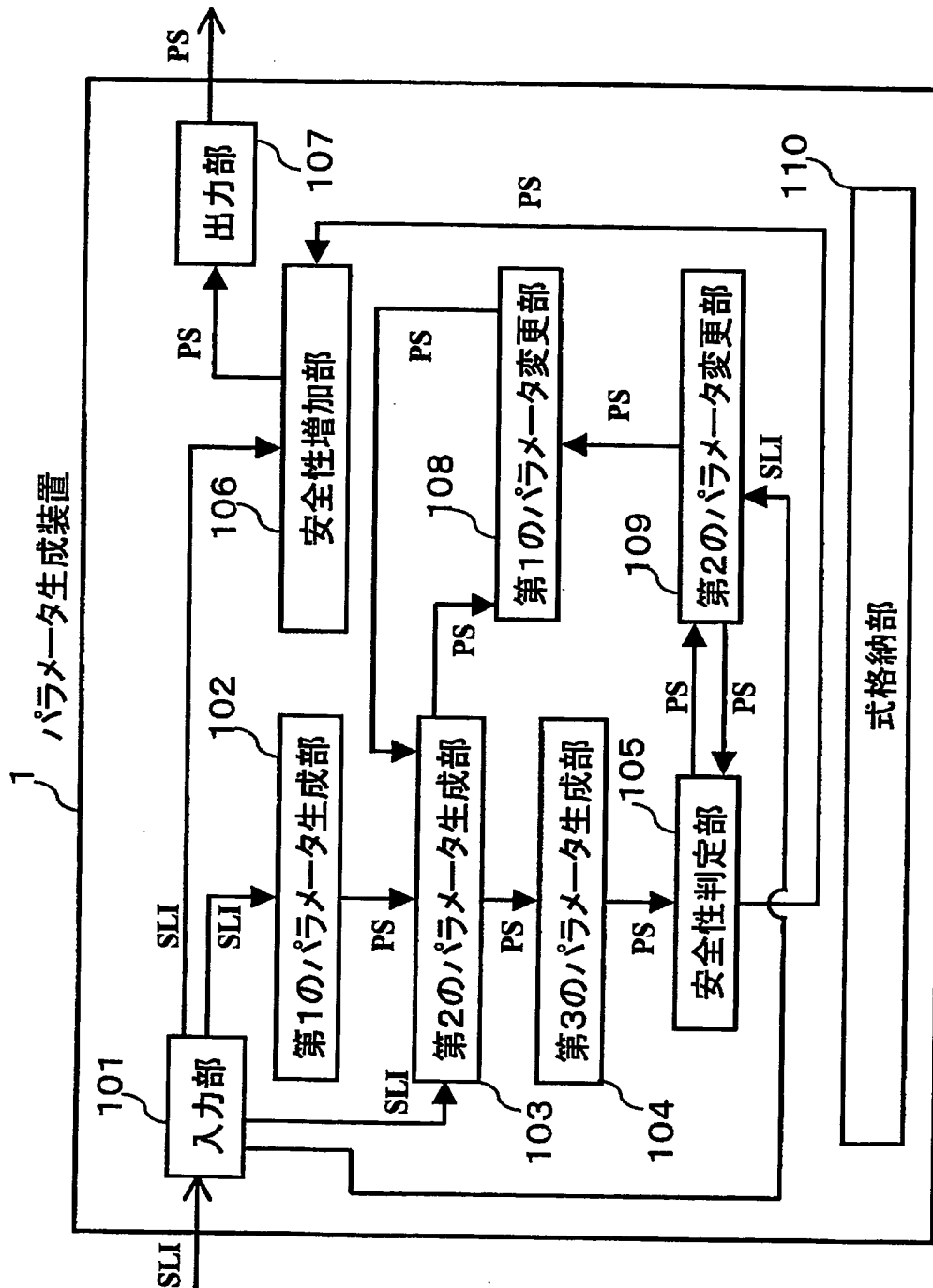
【符号の説明】

- 1 パラメータ生成装置
- 2 パラメータ変換装置
- 3 暗号システム
- 31 暗号装置
- 32 復号装置
- 33 通信路
- 101, 101b 入力部
- 102 第1のパラメータ生成部
- 103, 103b 第2のパラメータ生成部
- 104, 104b 第3のパラメータ生成部
- 105 安全性判定部
- 106 安全性増加部
- 107 出力部
- 108 第1のパラメータ変更部
- 109 第2のパラメータ変更部
- 110 式格納部
- 311, 321 パラメータ記憶部
- 312 公開鍵記憶部
- 313 暗号化部
- 322 鍵生成部
- 323 秘密鍵記憶部
- 324 復号化部

【書類名】

図面

【図 1】



【図 2】

パラメータN	解読時間T(秒)
70	16.587
72	18.68
74	26.497
76	25.869
78	31.182
80	37.76
82	56.442
84	56.359
86	68.174
88	86.6
90	111.78

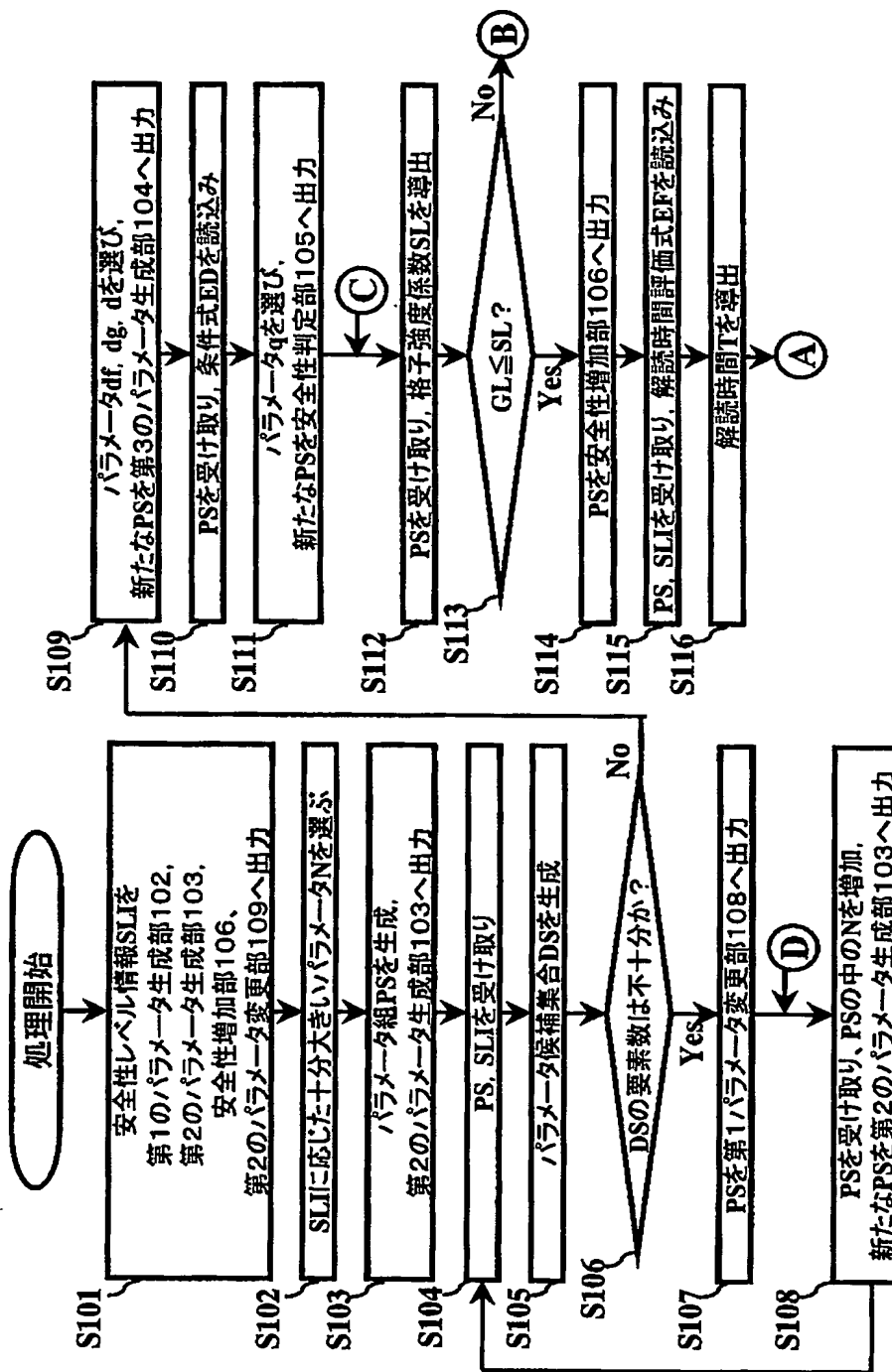
【図 3】

式格納部110

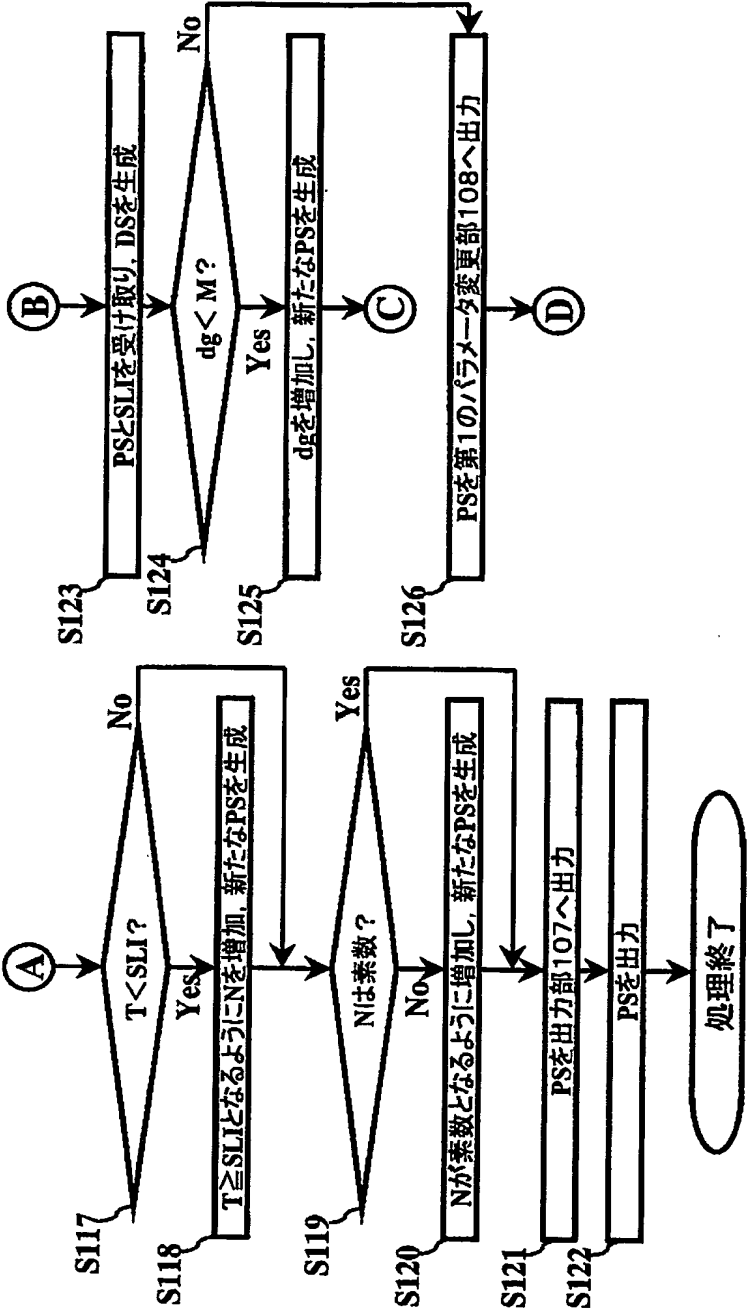
格子強度係数GL	2.12
解読時間評価式EF	$\log(T) = 0.04N - 6.2$
条件式ED	$6d + 2df - 1 < q/2$

初期安全性決定式IF	$\log(T) = 0.2002N - 18.884$
------------	------------------------------

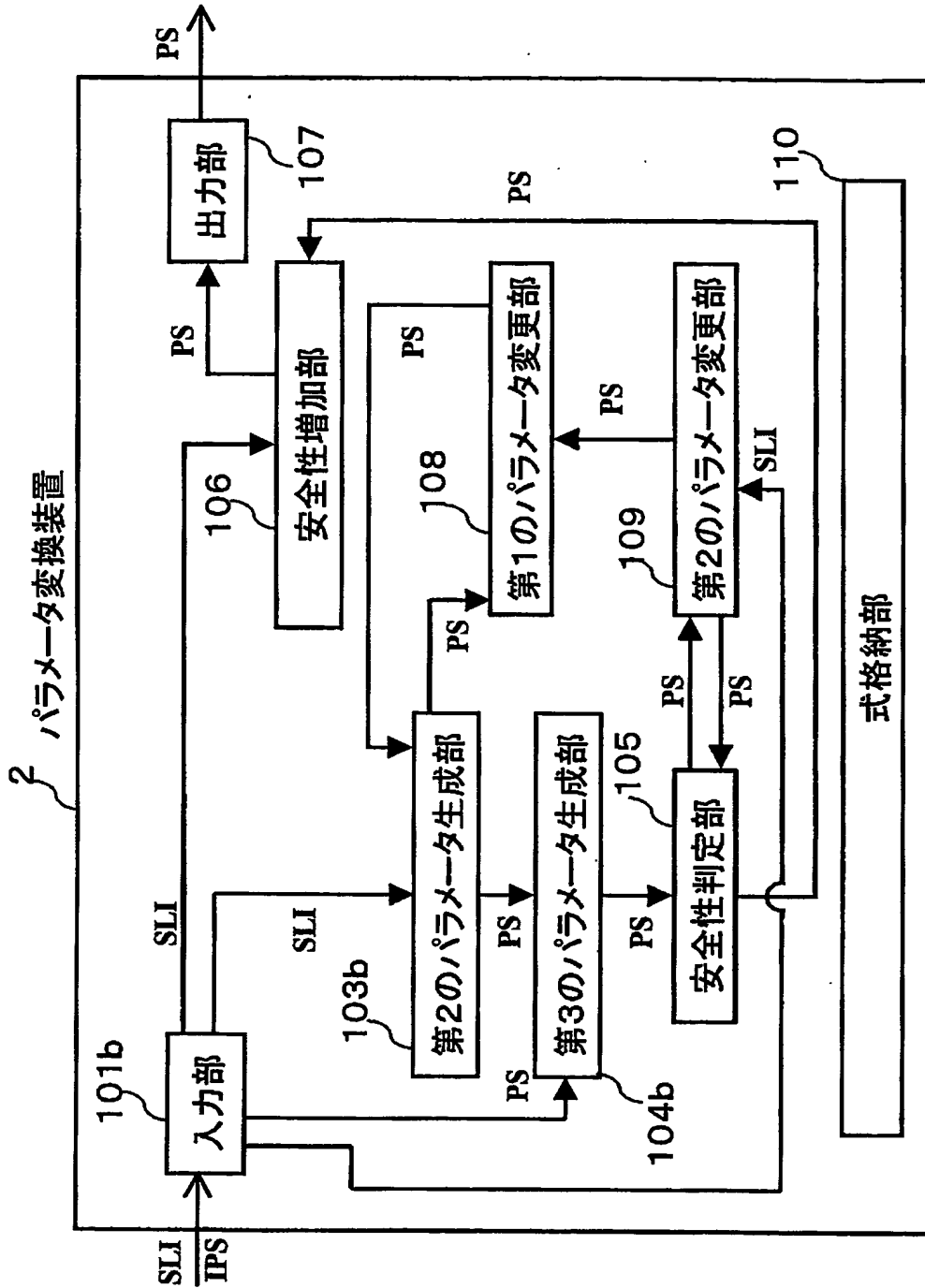
【図 4】



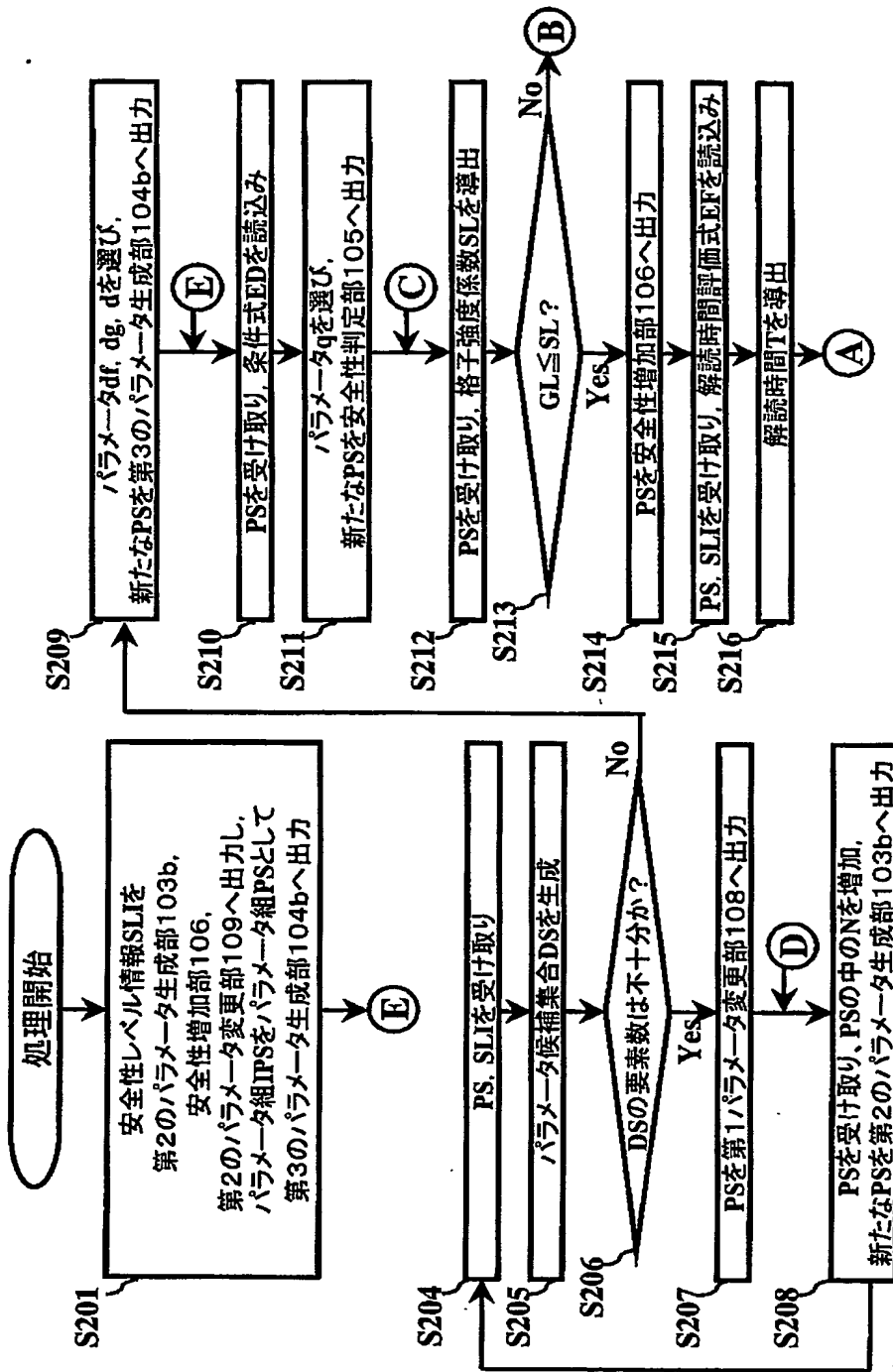
【図 5】



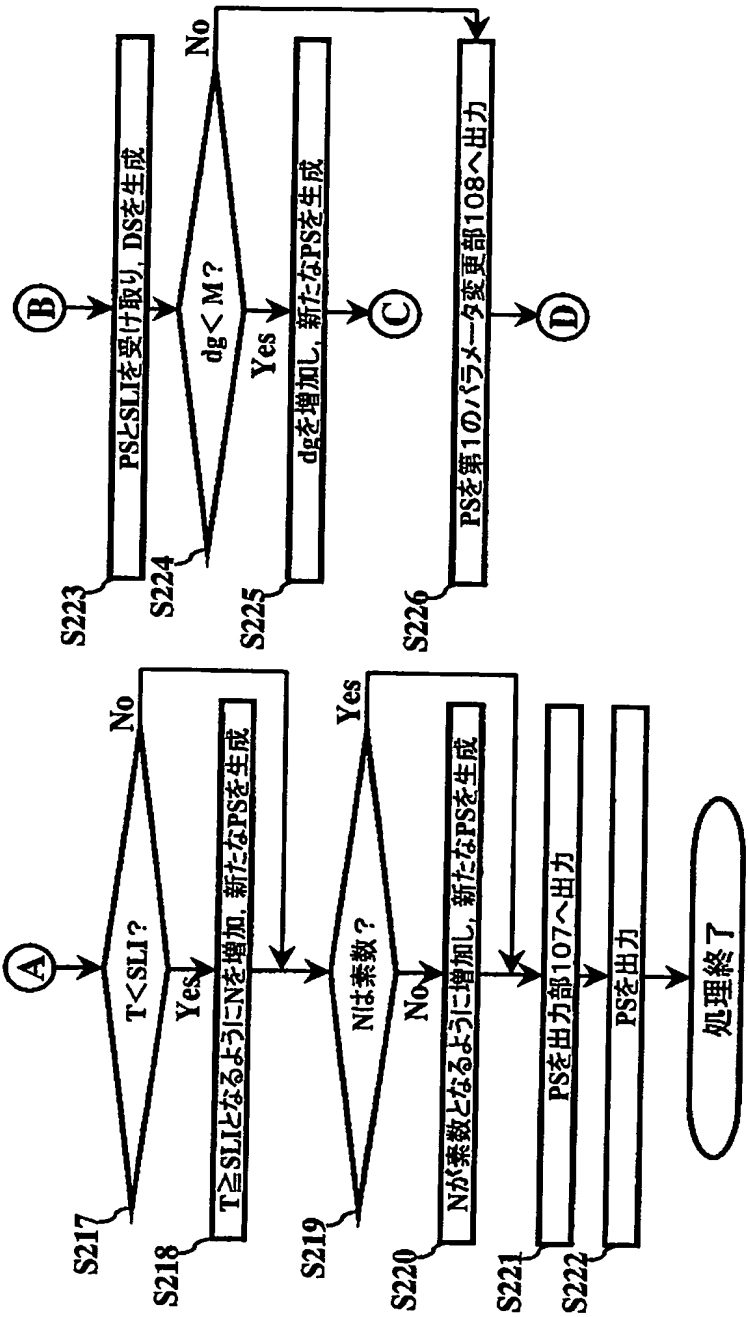
【図6】



【図 7】



【図 8】



【図 9】

安全性レベル情報SLI	パラメータ組IPS
512bit RSA暗号相当	IPS=(167,3,128,61,280,18)
1024bit RSA暗号相当	IPS=(263,3,128,50,24,16)
2048bit RSA暗号相当	IPS=(503,3,256,217,72,55)
:	:

【図 10】

式格納部 110

格子強度係数GL	2.12
解読時間評価式EF	$\log(T) = 0.04N - 6.2$

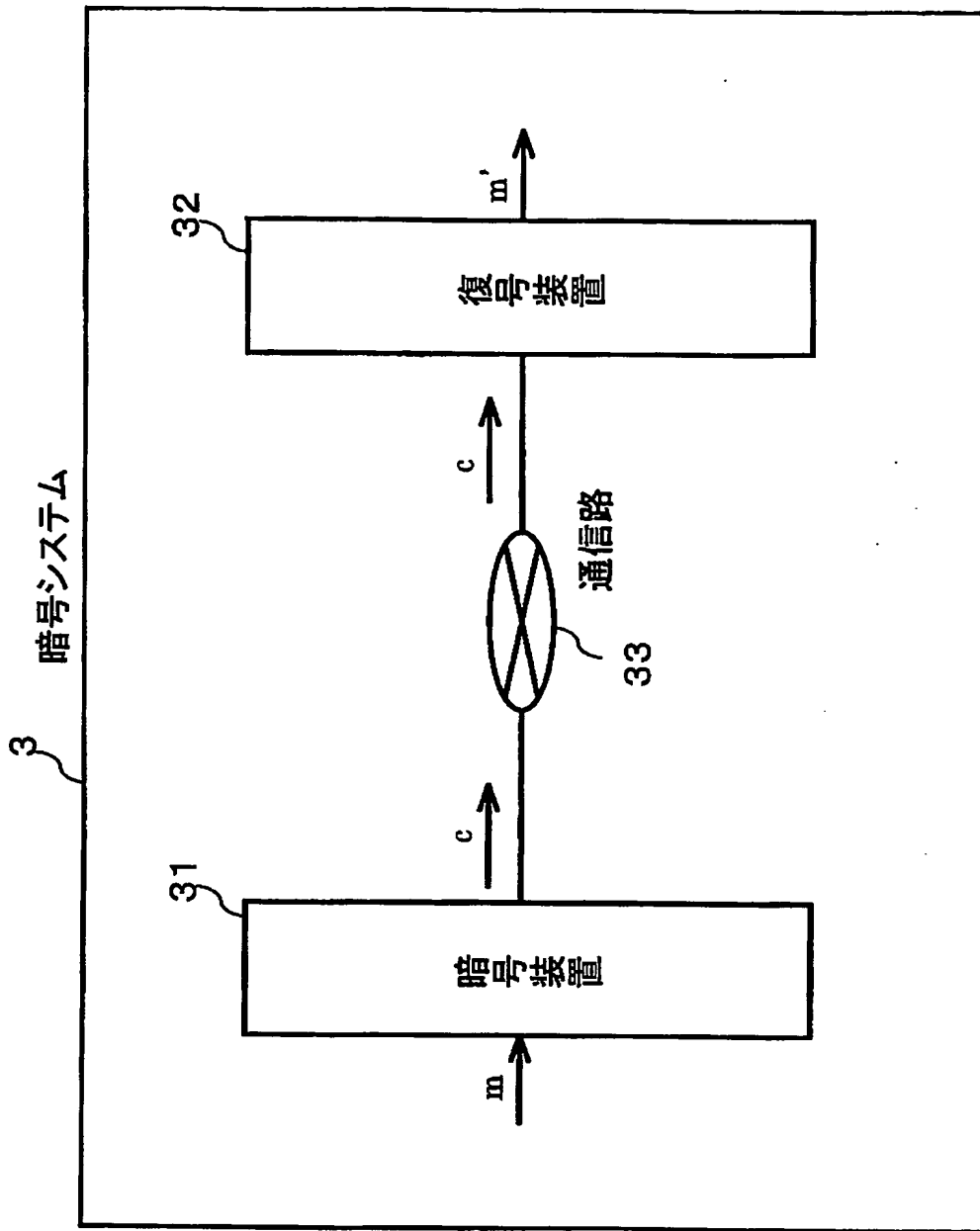
格子強度係数GL	3.5
解読時間評価式EF	$\log(T) = 0.08N - 4.8$

格子強度係数GL	4.6
解読時間評価式EF	$\log(T) = 0.13N - 4.4$

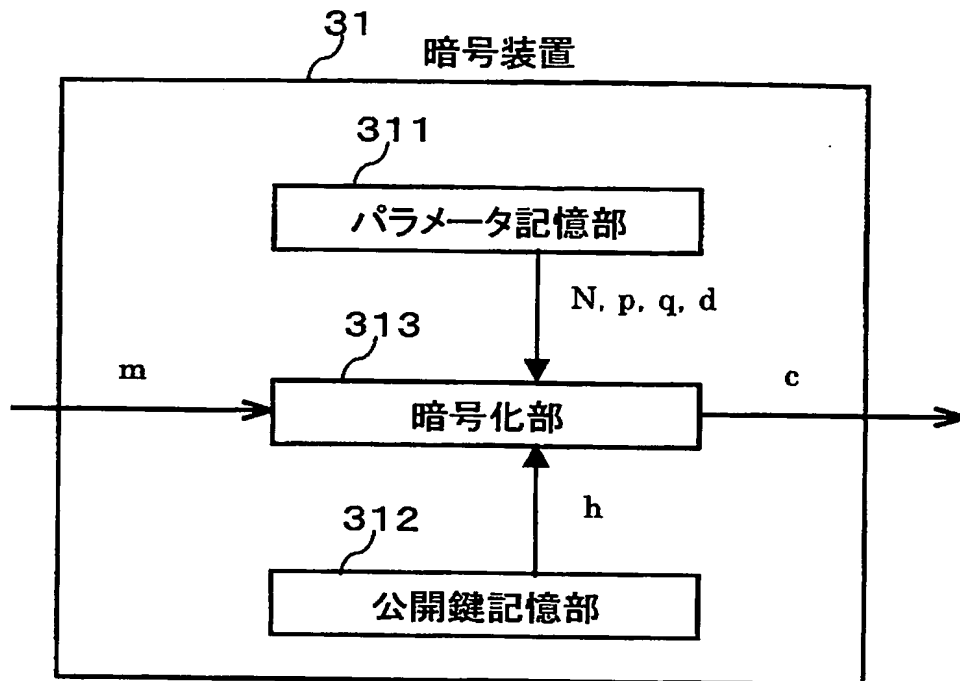
条件式ED	$6d + 2df - 1 < q/2$
-------	----------------------

初期安全性決定式IF	$\log(T) = 0.2002N - 18.884$
------------	------------------------------

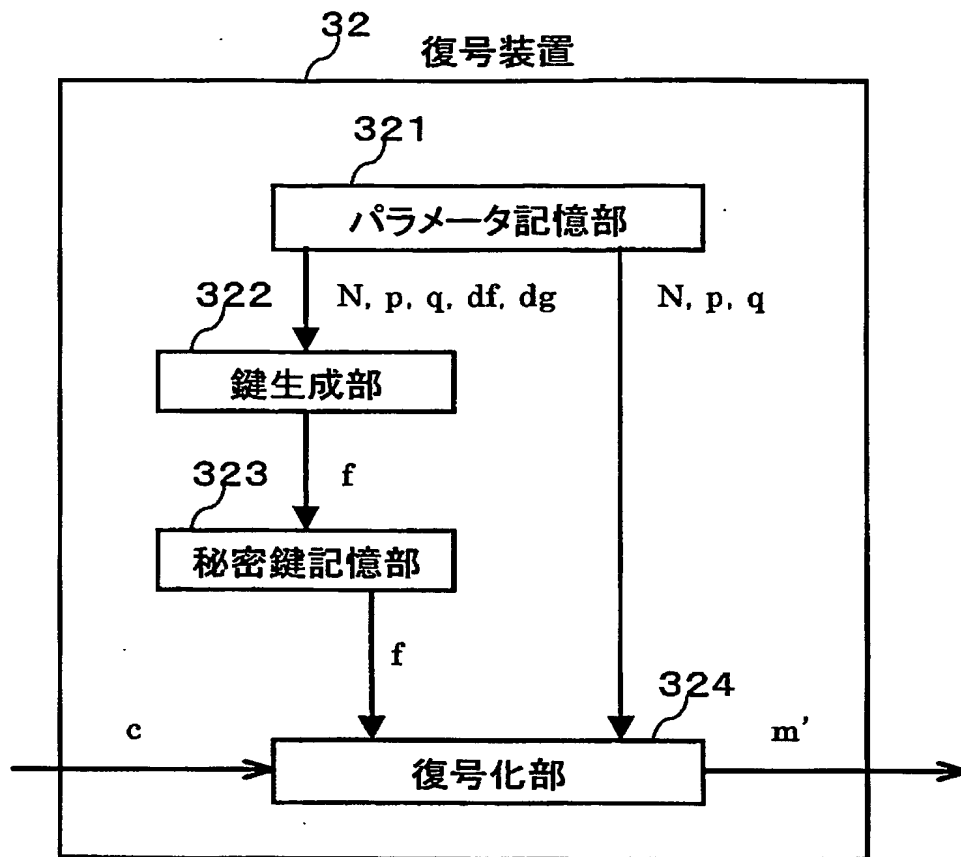
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないNTRU暗号のパラメータを生成するための条件が知られておらず、そのようなNTRU暗号のパラメータを生成できない。

【解決手段】 外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないNTRU暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、格子強度係数と安全性レベル情報に基づき、仮パラメータ組から出力パラメータを生成する出力パラメータ生成部とを備える。

【選択図】 図1

特願 2 0 0 3 - 1 1 9 9 7 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社